



Policy: NPRC-5015: Technology Resources
Acceptable Use Policy
Origination: 1-16-2019
Approved: 02-15-2019
Effective: 02-15-2019
Reviewed:
Last Updated:

Subject: Technology Resources Acceptable Use Policy

1. PURPOSE

The purpose of this policy is to establish parameters for the use and operation of Northern Pennsylvania Regional College (NPRC or the College) computing systems, telecommunications facilities, and network resources.

2. SCOPE AND APPLICABILITY

This policy applies to all computer users at NPRC including, but not limited to, guests, users, staff, faculty, and external entities.

3. REFERENCES

- 3.1 INDX-0010 Master Policy Index
- 3.2 FORM-5015 Technology Resources Acceptable Use Form
- 3.3 NPRC-2110 Employee Code of Conduct
- 3.4 NPRC-3235 Behavioral Code of Conduct for Students
- 3.5 Pennsylvania Right-to-Know statute, 65 P.S. 67.101
http://www.oca.state.pa.us/information_links/OCARTK.html

4. DEFINITIONS

- 4.1 Access is to approach or use an information resource.
- 4.2 For the purposes of this policy, the term Equipment shall refer to a laptop, power cord, charging brick and, in some instances, protective case assigned or loaned to a User.
- 4.3 The Director of Information Technology is the person responsible for the College's information resources.

- 4.4 For the purposes of this policy, the term User shall include the following: faculty, staff, employees, students, contractors, subcontractors, employees of contractors, volunteers, business associates, and any other persons who are determined and notified by the College to be subject to this policy. This definition does not create any additional rights or duties.
- 4.5 A Password is a string of characters known to a computer system or network and to a User who must enter the Password to gain access to an information resource.
- 4.6 Security represents those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

5. POLICY

- 5.1 The NPRC computing, telecommunications and networking resources are provided for the support of the instructional, research and administrative activities of the College. Use of these resources is a privilege granted by the College and it reserves the right to limit, restrict or extend access to these electronic resources.
- 5.2 Users are expected to conduct their activities within the restrictions and overall policies of NPRC, the laws of the Commonwealth of Pennsylvania and federal statutes. Agreement to abide by this policy and applicable statutes is a condition of acceptance to use the College's electronic resources and violators are subject to suspension of computer privileges and possible referral to the appropriate judicial or disciplinary process.
- 5.3 While the College recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, **there should be no expectation of privacy of information stored on or sent through College-owned information technology**, 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.*).
- 5.4 Information stored by the College may also be viewed by technical staff working to resolve technical issues.
- 5.5 The use of computer systems, telecommunications facilities, networks or other electronic resources of the College for the following purposes is deemed unacceptable:
 - 5.5.1 To perform Non-College-related political or charitable activities;

- 5.5.2 For commercial uses including, but not limited to, the promotion of "for profit" and/or privately-owned businesses or sale of private property;
 - 5.5.3 To abuse, defame, harass, or threaten another individual or group;
 - 5.5.4 To commit fraud or distribute any unlawful message(s);
 - 5.5.5 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
 - 5.5.6 Other unauthorized acts or actions not in accordance with College policies or not in the best interests of NPRC.
- 5.6 College data and resources must be protected to ensure the College's ability to meet its educational goals. Therefore, the following actions are prohibited:
- 5.6.1 Theft, damage or destruction of computing facilities, programs, or data;
 - 5.6.2 Access or use of computing facilities, programs or data that are not authorized to the User's account;
 - 5.6.3 Sharing usernames; passwords; pin numbers; or any other Security related procedures; files or accounts with other individuals, including, but not limited to, faculty, staff or administrators or students.
 - 5.6.4 Inhibiting or disrupting the operability of computer systems, telecommunications facilities, networks, or other electronic resources; and
 - 5.6.5 Intentionally introducing viruses, Trojan horses, worms or similar potentially damaging or harmful programs onto any College systems or networks.
- 5.7 NPRC respects and upholds the rights of holders of copyrights, their agents and representatives. It is the responsibility of Users to be aware of the rights of copyright owners. Legal use of copyrighted material can include, but is not limited to, ownership, license or permission, and fair use under the US Copyright Act. Illegal use includes:
- 5.7.1 Reproducing or allowing others to reproduce copyrighted software material in any form without proper authorization or taking actions not in keeping with federal and state copyright laws; and
 - 5.7.2 The use of software applications that allow for the direct sharing of music, movies, games, and software over the Internet when such peer-to-peer file

sharing contains copyrighted works without the permission of the copyright holder.

- 5.8 Virus protection software is included on all College computing devices. It is the end User's responsibility to
 - 5.8.1 Maintain the virus protection software by periodically scanning the User's computer; and
 - 5.8.2 Ensure that virus protection and security updates are provided by the maintenance contractors of any specialty electronic system that utilizes a computer-based operating system, including, but not limited to, copiers, document imaging systems and ITV systems.
- 5.9 All students and employees are given 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. With respect to those email accounts:
 - 5.9.1 It is the responsibility of the email account owner to delete unwanted messages and attachments and to otherwise maintain their account;
 - 5.9.2 Email can easily be forwarded to non-college accounts by the account owner; however, the account owner is responsible for the receipt of all information, including attachments, forwarded to another account;
 - 5.9.3 It is expected that students and employees will check their NPRC email accounts and the EmpowerSIS portal on a frequent and consistent basis; and
 - 5.9.4 Faculty should expect that students are accessing official electronic communications for the purposes of coursework.
- 5.10 Students found to be in violation of this policy may be subject to disciplinary action including, but not limited to, suspension of access to technology resources. Refer to NPRC-3235.
- 5.11 All students must acknowledge the receipt of Form-5015 Technology Resources Acceptable Use upon registration.
- 5.12 Employees found to be in violation of this policy may be subject to disciplinary action commensurate with the extent of the violation. Refer to NPRC-2110.
- 5.13 All Employees must acknowledge receipt of Form-5015 Technology Resources Acceptable Use during the employment intake process.

6. RESPONSIBILITIES AND TIMELINES

- 6.1 All Users of NPRC technology resources are responsible for adhering to this policy.
- 6.2 The Registrar or designee is responsible for collecting student acknowledgement of receipt of Form -5015 Technology Resources Acceptable Use Statement upon registration and annually as acknowledgement of said Policy.
- 6.3 The Vice President for Finance and Administration or designee is responsible for collecting employee acknowledgement of receipt of Form -5015 Technology Resources Acceptable Use Statement upon hiring.
- 6.4 The Vice President for Finance and Administration is responsible for the administration of this policy.

7. REVIEW STATEMENT

- 7.1 This policy shall be reviewed on a regular basis at least once every five years per the Policy Review Schedule established by the President or his designee. A review of the policy may be requested prior to the timeframe outlined by the policy review schedule by any student, faculty, staff, administrator, or board member. Such a request must be submitted in writing to the office of the President and must address specific concerns. Upon receipt of such a request, a complete review of the policy will be conducted within three months. Upon review, the President or President's designee may recommend to the Board of Trustees that the policy be amended or repealed.

8. SIGNATURES

Signature on file

Chair, Board of Trustees

Date

Signature on file

President

Date

Attachments: None

Distribution: Board of Trustees; regionalcollegepa.org

Revision Notes: Policy in Origination