NORTHERN PENNSYLVANIA REGIONAL COLLEGE	Policy: NPRC-5017: Email Management Origination: 1-16-2019 Approved: 04-12-2019 Effective: 04-12-2019 Reviewed: Last Updated:

Subject: Email Management

1. PURPOSE

The purpose of this policy is to establish parameters for appropriate use and operation of Northern Pennsylvania Regional College (NPRC or the College) email accounts and to ensure that users understand their responsibilities for protecting confidential data from breaches and safeguarding the College's reputation and proprietary and confidential information.

2. SCOPE AND APPLICABILITY

This policy applies to all individual who are assigned or given access to College email account(s), including an individual, department, or other group account.

3. REFERENCES

3.1 INDX-0010 Master Policy Index

3.2 NPRC-2110 Employee Code of Conduct

3.3 NPRC-3235 Behavioral Code of Conduct for Students

3.4 Pennsylvania Right-to-Know statute, 65 P.S. 67.101 http://www.oca.state.pa.us/information_links/OCARTK.html.

4. DEFINITIONS

4.1 For the purposes of this policy, the term User shall include faculty, staff, administrators, 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.

4.2 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.

4.3 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.

4.4 Spam messages are irrelevant or inappropriate messages sent on the Internet to many recipients.

4.5 Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

4.6 Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

4.7 Clickbait is Internet content which is designed to attract attention and encourage visitors to click on a link to a web page.

5. POLICY

5.1 Use of assigned college email accounts should be primarily for NPRC-related purposes.

5.2 Official electronic communication between college personnel and students shall occur using college-assigned email accounts.

5.3 Users shall be granted 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 by 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, including, but not limited to, email communication, may be viewed by technical staff working to resolve technical issues.

5.5 Users may not use their college-assigned email accounts to

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

5.5.2 Send unauthorized marketing content or solicitation emails;

5.5.3 Register for a competitor’s services unless authorized;

5.5.4 Send insulting or discriminatory messages and content; or

5.5.5 Intentionally Spam other people’s emails, including their coworkers.

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

5.6.1 Communicating with current or prospective students or partners;

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

5.6.3 Sharing their email address with attendees at conferences, career fairs, and other events.

5.7 Non-student Users may use their College email for personal reasons, including to

5.7.1 Register for classes or meetings;

5.7.2 Send emails to friends and family provided the User refrains from generating spam or disclosing confidential information; or

5.7.3 Download e-books, guides, and other content for personal use provided the content is safe and appropriate and does not interfere with the ordinary function or use of their assigned device(s).

5.8 To protect the College from hacker attacks, confidentiality breaches, viruses and other Malware associated with the use of email accounts, Users are required to

5.8.1 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);

5.8.2 Keep Passwords secret by remembering them instead of writing them down; and

5.8.3 Change Passwords at a minimum of every six months.

5.9 To protect the College from Malware or Phishing attempts, Users are required to

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

5.9.2 Avoid opening Clickbait titles;

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

5.9.4 Avoid opening or acting upon emails with inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive exclamation marks); and

5.9.5 Report all suspicious emails to the Director of Information Technology.

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

5.11 Faculty and Staff Users are to use the supplied approved email signature. The template for the approved signature may be obtained from the Director of Technology Service or the Marketing and Public Relations Coordinator.

5.12 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.

5.13 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.

6. RESPONSIBILITIES AND TIMELINES

6.1 All Users of the NPRC email system are responsible for adhering to this policy.

6.2 The Director of Information Technology is the person responsible for responding to reports of suspicious emails and other activities associated with maintenance and security of the College's information resources.

6.3 The Vice President for Finance and Administration is responsible for the administration of this policy.

7. REVIEW STATEMENT

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; www.regionalcollegepa.org
Revision Notes: Policy in Origination