Email Policy

Policy Number: 505

Categorized: Information Technology

Responsible Office: VP of Information and Engineering Technologies and College Computing

Subject: Policy and procedures governing the use of College email

Related Policies: Electronic Communications and Social Media Policy, Security Awareness Training Policy

Procedures: N/A

Additional Information:

Effective Date:

Last Reviewed Date: 03/15/2021

---

1. Scope

This policy applies to all Northern Virginia Community College (NOVA) employees, including full and part-time staff, faculty, contractors, consultants, volunteers, interns, student hires, retirees and students (collectively, "users").

2. Policy Statement

Northern Virginia Community College grants users access to College email in order to perform their authorized functions. Users are required to abide by the following policies:

Authorized Use of Email

a. Access to electronic mail is an essential tool that imposes on users certain accompanying responsibilities. The Information Technology – Employee Acceptable Use Agreement, the M365 Acceptable Use Agreement, and the Information Technology Employee Ethics Agreement; NOVA, VCCS, and DHRM polices; and the same standards of conduct that are expected of students, faculty, and staff regarding the use of other College facilities, services, and resources apply to the use of electronic mail.

b. All faculty, staff and students are expected to check their College email on a frequent and consistent basis in order to ensure that they are staying current with all official communications.

c. Though college email is for official use, college electronic mail services may be used for incidental personal purposes provided that such use does not directly or indirectly interfere with the College operation of computing facilities or electronic mail services or interfere with the user's employment or other obligations to the College. There should be no expectation of privacy in regard to electronic mail messages of a personal nature sent or received from College email accounts or from College computers.

d. Official email that contains personal or sensitive information sent to registered students should only be sent encrypted to NVCC or VCCS student email addresses. Email to a non-NVCC or non-VCCS student email address cannot contain any information protected under FERPA.
e. Other communication of a more general nature that does not include legally required, personally identifiable, or FERPA-protected information should use the most appropriate electronic means for reaching the intended audience. This includes general information about class assignments, quizzes, tests, programs, college-wide announcements, financial aid or tuition payment due dates, course or registration information, weather-related closings or delays, and college events.
f. Where a prospective student does not have a VCCS email address, the email address provided by the student may be used.

Safety and Security

a. Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized. Each user is responsible for all electronic mail transactions made under the authorization of his or her ID.
b. Faculty and staff may not set up their college email account to automatically forward email to an email account outside the college.

Access to and Disclosure of Email

a. Employee email is subject to the Freedom of Information Act.
b. The College has the right, consistent with this policy and applicable law, to access, review and release all electronic information that is transmitted over or stored in College Systems or facilities, whether or not such information is private in nature, and therefore, confidentiality or privacy of electronic mail cannot be guaranteed.
c. Employees who resign or terminate employment will have their email accounts terminated. Such employees should be aware that their email accounts will be accessed by their supervisors in order to continue to conduct College operations after they leave. If such access is necessary, the appropriate Administrative Council member must make this request through Human Resources before access will be granted.
d. Retirees are eligible to retain email accounts and must complete security awareness training on an annual basis to maintain access to a college email account.

Prohibited Use

a. Using electronic mail for illegal activities is strictly prohibited.
b. College electronic mail services may not be used for non-college commercial activities, personal financial gain, non-approved charitable activities, or for the advancement of any political agenda.
c. Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the College or any unit of the College unless expressly authorized to do so.
d. College email services may not be used for purposes that could reasonably be expected to cause, (directly or indirectly) strain on any computing facilities, or interference with others' use

of electronic mail or electronic mail systems. Such uses include, but are not limited to, the use of electronic mail services to:

i. Send or forward chain letters. These emails often contain warnings that may very well be hoaxes. Use appropriate websites, like http://www.snopes.com/, to validate the myths and warnings.
ii. "Spam" – that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail.
iii. "Letter-bomb" – that is, to resend the same email repeatedly to one or more recipients.
iv. Knowingly send or transmit computer viruses

e. The email system should not be used to store documents or email messages that are the basis for official action, historical record, or truly official communication. If a particular email needs to be saved for official document retention purposes, it should be printed or saved as a separate document.

3. Definitions

Personal use: use that is not job-related.

Official Information/Communications: messages and information sent from college offices, faculty and/or administrators regarding services, programs and other relevant information.

4. Procedures

N/A

5. Authority

VCCS IT Policy 20.1 – Microsoft 365 Account Security

VCCS IT Policy 20.2 – Microsoft 365 Email Services Security

VCCS IT Policy 20.5 – Microsoft 365 On-Premises Security

VCCS IT Policy 20.6 – Microsoft 365 Security Monitoring

Information Security Requirements 6.0, Email Accounts

DHRM Policy 1.75 Use of Electronic Communications and Social Media