Christopher Newport University

Policy: Acceptable Use of Computing Resources Policy
Policy Number: 6010

Executive Oversight:	Vice President for Finance and Planning/CFO
Contact Office:	Information Technology Services
Frequency of Review:	Annually
Date of Last Review:	August 2021

A. PURPOSE

This policy establishes the terms of use for University communication and computing resources.

B. POLICY STATEMENT

All Christopher Newport University communication and computing resources are University property. No user of Christopher Newport's communication or computing resources has any expectation of privacy or confidentiality in any material, data, file or communication that in any way makes use of these University resources.

All use of communication and computing resources by employees is also governed by the Virginia Department of Human Resource Management Policy: 1.75 – Use of Electronic Communications and Social Media which can be found at:
https://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf

These resources represent a substantial investment of public dollars. They are finite and intended to be used in support and advancement of Christopher Newport University's mission, purposes and activities by authorized users. Use of these resources is a privilege that is extended to students, employees, contractors and visitors upon specific terms.

C. DEFINITIONS

University Communication and Computing Resources: Any and all computer and network equipment, networks, devices, systems, databases, installed applications, access to the internet, and use of University email services.

Users: Employees, students, contractors, consultants, volunteers, and visitors authorized to use University communication and computing resources.

D. PROCEDURES

Any and all use of Christopher Newport's communication and computing resources must at all times conform to state and federal law, and to all applicable University policies and codes of conduct. Any conduct that is prohibited generally, is prohibited equally when it is accomplished by or through use of University communication or computing resources. Prohibited conduct includes but is not limited to:

- Accessing, uploading, downloading, transmitting, printing, posting or storing information with sexually explicit content prohibited by law (e.g. see *Code of Virginia* § 2.2-2827);

- Accessing, uploading, downloading, transmitting, printing, posting, or storing fraudulent, threatening, obscene, intimidating, defamatory, discriminatory, or otherwise unlawful messages or images;

- Accessing, uploading, downloading, transmitting, printing, communicating or posting access-restricted university information, data or records, except as necessary to perform legitimate university activities;

- Any activity intended to disable or circumvent Christopher Newport's physical or electronic security measures, without authorization by the Information Security Officer (ISO) or Chief Information Officer (CIO);

- Any activity that burdens any system or other resource in a manner that limits the availability of resources to other users, or modifies its intended use; and

- Installing or downloading any new software, whether free or purchased, onto a university computer without: i) express permission from the ISO; or ii) pursuant to administrator rights approved by a Vice President for a particular limited purpose or purposes.

University communication and computing resources are protected by a system of electronic authentication and authorization procedures that rely on user passwords and usernames ID's (together referred to as access credentials) for validation. Authorized users are assigned personal access credentials. Personal access credentials must be kept confidential and users shall not share them. Users shall not use personal access credentials other than their own, unless authorized to do so for a legitimate University purpose. Users are responsible for any and all activity enabled by their personal access credentials, except where it can be established that the credentials were stolen. Users must take every reasonable precaution against theft of their personal access credentials.

Christopher Newport University monitors and may access any and all files, data, and materials stored, generated, or transmitted by or through University computers, networks, or electronic devices, without notice to the user, as deemed necessary to enforce these terms of use, any other University policy, rule or regulation, or the civil or criminal law. Such access must be approved by the appropriate vice president in consultation with University Counsel and ITS shall maintain a log of all requested searches and action taken. In addition, Christopher Newport may take any action necessary to repair, maintain or upgrade equipment, systems and data.

Violations of this policy shall be reported to Information Technology Services through the Information Security Officer or the Chief Information Officer. ITS shall share the report with Human Resources, the Provost, or Vice President for Student Affairs, as appropriate.

Any violation of this policy or other University policies, rules or regulations or of the law, through or by use of University communication or computing resources may result in limitation or termination of use privileges, in addition to prosecution or student/employee discipline.

E. REFERENCES

Virginia Department of Human Resource Management Policy: 1.75 – Use of Electronic Communications and Social Media:
https://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf

VITA SEC 501– IT Information Security Standard
https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

DHRM Standards of Conduct 1.60
http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol1_60.pdf

University Handbook

F. APPROVAL AND REVISIONS

Approved by: Policy Committee, November 29, 2017

Revision 1: Policy Committee, March 22, 2019
Revision 2: Policy Committee, March 4, 2020
Revision 3: Policy Committee, August 25, 2021

G. NEXT REVIEW DATE: Fall 2022