# Duke Acceptable Use Policy

IN THIS SECTION

‹ Security Program ‹ Duke Acceptable Use Policy

Applicable To:

Duke University

Version 2.0

## Authority

Duke University Chief Information Officer
Duke University Chief Information Security Officer

## Introduction

Duke cherishes freedom of expression, the diversity of values and perspectives inherent in an academic institution, the right to acknowledgment, and the value of privacy for all members of the Duke community. At the same time, Duke may be required by law to access and disclose information from computer and network users[1] accounts or may find it necessary do so in order to protect Duke's legal interests, uphold contractual obligations, or comply with other applicable Duke policies. Duke may also be required to access

information to diagnose and correct technical problems.

## Scope

Under some circumstances, as a result of investigations, subpoenas, lawsuits or threatened litigation, Duke may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources ("information records"). In the rare cases where Duke determines that a review of information records is needed but not legally compelled and the President and EVP give explicit approval, Duke may, in its reasonable discretion, conduct such a review. In addition, system failures may lead to loss or exposure of data, so users should not assume that their messages and files are secure. For these reasons, the ultimate privacy of messages, network transmissions and files cannot be ensured[2].

An account owner should not reveal a password to an IT support technician or any other individual, even though they may claim to work for the IT service (over the phone or in person). If, in the professional judgment of the user, it is necessary to share a password with an IT support technician or any other individual, the password must be changed as soon as possible thereafter. Once shared, a password is considered compromised and must be changed immediately.

Neither Duke nor its agents restrict the content of material transported across its networks. While Duke does not position itself as a censor, it reserves the right to limit access to its networks or to remove material stored or posted on Duke computers when applicable Duke policies, contractual obligations, or state or federal laws are violated. In addition, users bear a personal responsibility to comply with all Duke policies, contractual obligations, and state and federal laws and regulations, including protecting the private information of others. Alleged violations will receive the same due process as any other alleged violation of Duke policy, contractual obligations, or state or federal laws.

---

[1] N.B. The Acceptable Use Policy was first drafted in 1995-96, and this updated version was ratified by the Duke University Academic Council in 2005. The current Acceptable Use Policy

was ratified on Sept. 10, 2010, by the Information Security Steering Committee as applying to all members of Duke University (including the School of Medicine and Nursing) and its affiliated entities with the exception of the Duke University Health System. Review and ratification by DUHS is pending and may require development of a separate protocol in the clinical setting for electronic Protected Health Information (ePHI).

[2] Unless the legal or practical circumstances of the situation do not permit it, University Counsel will take appropriate steps to notify individuals when information records are preserved for e-Discovery, and prior to the access of those information records.

---

**Last Reviewed:** 11/18

**Document Type:** Policy