| Policy Title: Acceptable Use Policy for University Computers and Information Technology Systems | Approval Date: 09/03/09 |
|---|---|
| Policy ID: IT 5105 | Effective Date: 09/03/09 |
| Oversight Executive: VP for Information Technology & CIO | Review Date: 07-01-10 |

# 1. Purpose

Access to computer systems and networks owned or operated by Radford University imposes certain responsibilities and obligations and is granted subject to university policies, and local, state, and federal laws. This policy outlines the requirement and responsibilities of users to comply with the University's Acceptable Use Policy and the consequences of noncompliance with this policy. Radford's Acceptable Use Policy applies to any individual hereafter referred to as "users" using Radford University-owned or leased computers, networks, Internet connections, and communication systems transmitting either data, voice, or video information. All users of university information facilities have responsibility to use these systems in a respectful, ethical, professional, and legal manner.

# 2. Policy

- Users are responsible for all activity that occurs in or through their accounts and/or their computers, whether personally or University owned.
  - o Users shall not share access to individual accounts.
  - o Users shall follow the IT 5101 Password Policy.

- Users may only access information that is their own, information to which they have been given explicit documentable authorization to access, or public information.

- Users with access to personally identifiable, confidential, or sensitive information must follow guidelines in the IT 5102 Data Storage and Media Protection Policy to properly safeguard information and must not transmit unencrypted sensitive data over the Internet.

- Faculty and staff shall comply with Virginia Department of Human Resource Management Policy 1.75 – Use of Electronic Communications and Social Media.

- Users shall not install or remove software or hardware on Radford University owned systems that adversely affects the security, integrity and/or performance of the university systems and data.

- Users shall abide by all relevant state and federal laws governing copyrights, trademarks, licensing terms for corporate software, ownership of information, and related material.
  - o Users are prohibited from engaging in any illegal activities such as software piracy through either distribution of copyrighted software or illegal attainments of software or other copyrighted materials.
  - o Users are prohibited from engaging in any illegal peer-to-peer file sharing. Such activity is not only subject to state and federal penalties; it increases security risks for Radford University's network.

- To access copyrighted music, users should only access sites that provide such material legally.  Please refer to the CIO web site http://cio.asp.radford.edu for a listing of legal sources of copyrighted music.

- Users, in respect of the operation and integrity of a shared system, shall not attempt to interfere with the normal operation, integrity, validity, or the security of any university or non-university information system.
  - Users shall abide by the regulations posted in computer labs and on university systems.
  - Users shall not attempt to misappropriate or guess system passwords nor inappropriately use system accounts.
  - Users shall not use other computers or programs to decode passwords, access restricted system control information, or monitor restricted system or network communications.
  - Users shall not intentionally monopolize or waste resources such as Central Processing Unit (CPU) time, network bandwidth, disk storage, printers, paper, manuals, etc.
  - Users shall report possible security violations and/or problems to the university Information Security Officer (ISO).
  - Users shall assist university officials with the investigation of violations of university computing policies and will provide university officials with unencrypted files necessary for the investigation of violation of university computing policies. Failure to cooperate with such investigations will result in suspension of privileges and discipline under the Standards of Conduct.

- Users shall not use university systems to view, store or transmit obscene or pornographic material in violation of state and federal law.

- University information systems shall not be used for non-RU-affiliated, on-going commercial business enterprises or partisan political purposes or for any unauthorized mass mailings.

- Users shall not use university systems to abuse, verbally assault, defame, harass, intimidate, or otherwise annoy an individual or individuals.

- Users shall observe the conditions of the Radford University Privacy Statement when developing web pages and web applications. The Privacy Statement is found on the Radford University homepage.

- Users are responsible for following all RU IT Policies and all applicable federal and state policies.

The university reserves the right to seize the computer and examine/copy the files therin pursuant to any investigation of any alleged policy violation or violation of state or federal law, or pursuant to any university-related investigation.

Access to university information systems is a privilege that may be revoked for reasons including, but not limited to, violations of the Acceptable Use Policy for Computers and Information Technology Systems.  Access may be revoked on an interim basis by the university in order to safeguard university resources, to protect its network from systems and events that threaten or degrade operations, to limit the university's liability for damages due to violations of the Acceptable Use Policy, and to investigate allegations of abuse of the Acceptable Use Policy. Violation of this policy will be subject to disciplinary action as specified in the Teaching and Research Faculty, Administrative and Professional Faculty, Classified Staff, and Student Handbooks. Violators may also be subject to

prosecution under various relevant state and federal laws. The university disclaims all liability for harm or offense suffered as a result of the conduct or action of account holders of the university's information systems.

## 3. <u>Procedures</u>

## 4. <u>Definitions</u>

- Users – Anyone with an active account on a Radford University system.

## 5. <u>Related Information</u>

- CIO web site (http://cio.asp.radford.edu)
- IT Policies (http://cio.asp.radford.edu/policy/policy.aspx)
- IT 5101 Password Policy (http://cio.asp.radford.edu/policy/IT-5101-PasswordPolicy.pdf)
- IT 5102 Data Storage and Media Protection (http://cio.asp.radford.edu/policy/IT-5102-DataStorage.pdf)
- Virginia DHRM Policy 1.75 – Use of Electronic Communications and Social Media  Policy 1.75, Use of Electronic Communications and Social Media

## 6. <u>Policy Background</u>

## 7. <u>Approvals and Revisions</u>

Updated:  April 26, 2011 to reflect name change to DHRM policy 1.75, Use of Electronic Communications and Social Media

Approved September  3, 2009 by Radford University Cabinet