

Fuqua Acceptable Use Policy

1.0 Overview

The intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity at Duke University's Fuqua School of Business (noted as "Fuqua" for the rest of this document). Fuqua is committed to protecting Fuqua's employees, partners and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Fuqua. These systems are to be used for business purposes in serving the interests of the college, and of our faculty, staff and students (hereafter noted as "user" or "users") in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Fuqua employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Fuqua. These rules are in place to protect the user and Fuqua. Inappropriate use exposes Fuqua to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Fuqua, including all personnel affiliated with third parties, as well as students. This policy applies to all equipment that is owned or leased by Fuqua.

4.0 Policy

4.1 General Use and Ownership

1. While Fuqua's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Fuqua. Because of the need to protect Fuqua's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Fuqua.
2. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, users should be guided by departmental policies on personal use, and if there is any uncertainty, users should consult their supervisor or manager.
3. Fuqua recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Fuqua's Information Sensitivity Policy.
4. For security and network maintenance purposes, authorized individuals within Fuqua may monitor equipment, systems and network traffic at any time, per Fuqua's Audit Policy.
5. Fuqua reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by Duke University's confidentiality guidelines, details of which can be found in the Staff Handbook. Examples of confidential information include but are not limited to: Fuqua private, Fuqua strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Users should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed semi-annually; user level passwords should be changed every three months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
4. Use encryption of information in compliance with Fuqua's Acceptable Encryption policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by users from a Fuqua email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Fuqua, unless posting is in the course of business duties.
7. All hosts used by the user that are connected to the Fuqua Internet/Intranet/Extranet, whether owned by the user or Fuqua, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Fuqua-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Fuqua.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Fuqua or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Fuqua computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Fuqua account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not

- limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Fuqua is made.
 11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the user's normal job/duty.
 12. Circumventing user authentication or security of any host, network or account.
 13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
 14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
 15. Providing information about, or lists of, Fuqua users to parties outside Fuqua.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Fuqua's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Fuqua or connected via Fuqua's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.4. Blogging

1. Blogging by users, whether using Fuqua's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Fuqua's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Fuqua's policy, is not detrimental to Fuqua's best interests, and does not interfere with an employee's regular work duties. Blogging from Fuqua's systems is also subject to monitoring.
2. Fuqua's Information Sensitivity policy also applies to blogging. As such, Users are prohibited from revealing any Fuqua confidential or proprietary information, trade secrets or any other material covered by Fuqua's Information Sensitivity policy when engaged in blogging.
3. Users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Fuqua and/or any of its affiliates. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Duke University's Non-Discrimination and Anti-Harassment policy as detailed in the Staff Handbook.
4. Users may also not attribute personal statements, opinions or beliefs to Fuqua when engaged in blogging. If a user is expressing his or her beliefs and/or opinions in blogs, the user may not, expressly or implicitly, represent themselves as an employee or representative of Fuqua. Users assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Fuqua's trademarks, logos and any other Fuqua intellectual property may also not be used in connection with any blogging activity.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
------	------------

<i>Bloggng</i>	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
----------------	--

<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.
-------------	---

7.0 Revision History

Date	Who made the revision	Change made
2012-01-20	Fuqua Infrastructure	Initial issue

This document was adapted from a draft created by the SANS Institute and is used by permission of the SANS Institute.