Policy on Responsible and Ethical Use of Computing Resources

Final version, approved by the CIT October 26, 1998
Revisions approved by the CIT November 4, 2002
Revisions approved by IT Executive Committee (ITEC) January 8, 2016

1. Introduction

This policy is intended to promote the responsible and ethical use of the computing resources and computing systems of Wake Forest University. Copies of the policy shall be made available to all users of the University's computing resources and computing systems, and every reasonable effort shall be made to ensure that all users read the policy at least once.

The policy applies to all computer and computer communication systems owned, leased, operated, or contracted by the University. This includes, but is not limited to, tablets, personal computers, laptops, smart phones, computer networks, computer peripherals, and software, whether used for academic, administration, research, or other purposes. This also includes use of University data or access to computer systems by personal devices such as computers, tablets, and smart phones by faculty, staff, students and guests. The policy extends to any use of University systems to access computers elsewhere. For purposes of this policy, references to "computing resources" shall also include "computing systems."

The administrators of various on-campus and off-campus computing systems, and those responsible for access to those systems, may promulgate additional regulations to control their use, if not inconsistent with this policy. Administrators are responsible for publicizing any such additional regulations.

2. Basic Principles

The University's computing resources are for administrative, instructional, educational, and research use by the students, faculty, staff, vendors and contractors of Wake Forest University. Ethical standards which apply to other University activities (Honor Code, Social Regulations and Policies, and all local, state, and federal laws) apply equally to use of University computing resources.

As in all aspects of University life, users of the University's computing resources should act honorably and in a manner consistent with ordinary ethical obligations. Cheating, stealing, making false or deceiving statements, plagiarism, vandalism, and harassment are just as wrong in the context of computing resources as they are in all other domains.

Use of computing resources is restricted to authorized users. For the purposes of this policy, an "authorized user" is defined as an individual who has been assigned a login ID and authentication credentials such as password for use of computing resources. Authorized users are responsible for the proper use of the accounts assigned to them under their login ID and

authentication credentials. Users are responsible for all actions performed under their login ID, and sharing of authentication credentials, including passwords, is prohibited. The University may in its discretion take into consideration information indicating that a user's account has been compromised as a result of illegal activity by a third party when determining whether a user is in violation of this Policy. Users are also responsible for reporting any activities which they believe to be in violation of this policy, just as students are responsible for reporting Honor Code violations. Individuals may use only those computing resources they have been authorized to use. Use of these resources must be done:

- In a manner consistent with the terms under which they were granted access
- In a way that respects the rights of other users
- So as not to interfere with or violate the normal, appropriate use of these resources
- In a responsible manner and consistent with University policies and the workplace and educational environment.

For faculty, staff, vendors, contractors, and other non-students, limited personal use of University issued computing resources is authorized so long as it does not impact University computers, networks, or interfere with work related activities and is not prohibited by this or other policies.

For students, personal activity is allowed as long as it does not interfere with other University computers or network bandwidth and is not prohibited by this or other policies.

3. System Monitoring

This statement serves as notice to all users of campus computing resources that regular monitoring of system activities occurs and users should have no expectation of privacy while on the WFU network or computer systems. This monitoring is to provide for the security and integrity of University data and systems and is in no way judgmental on computer usage. Any data collected during monitoring may be shared with appropriate parties as required for business purposes or as required by law.

Only people engaged in supporting University computing resources are authorized to perform monitoring of systems and only for systems under their control. This includes but is not limited to:

- Administrators of operating systems, networks, web sites, and applications. This includes:
    - Centralized IT staff in the Information Systems (IS) department
    - Decentralized IT sections such as those in the School of Business, Advancement, Athletics, Law School, and Faculty Instructional Technology Group (ITG)
    - Desktop support personnel

In addition, the following departments are authorized to monitor any and all WFU computing resources:

- Audit and Compliance Department
- Information Systems Information Security Department.

Monitoring may include but may not be limited to the following:

- Any system log files which contain information pertaining to processes executed on a given system.
- System directories, temporary storage areas, work areas, and all areas *outside* of users' personal files. (Personal files are defined as any files created by and/or owned by the user and may be work related or non-work related.)
- Network traffic and utilization, both Internet and intranet.
- Unsuccessful attempts to log into an account or a network.
- Attempts to gain unauthorized access to departmental or personal computers, files or data within the campus community.
- Attempts to disguise the user's identity or the source of electronic mail.
- Any activity which in the opinion of any of the above-mentioned staff potentially compromises the security or integrity of any computing resource.

During any monitoring, it is possible that the monitoring staff may see user activity such as:

- Websites visited
- Emails
- Office files such as Word, Excel, PowerPoint, etc.
- Virus related information or files
- Pictures and videos

Any data collected during monitoring may be used for purposes outlined in this policy and may be destroyed when no longer needed for such purposes and when permitted by law.

Examples of monitoring:

1. WFU is notified by law enforcement or other competent authority of a list of Internet websites whose main purpose is to hack users that navigate to the site. Information Security reviews the web sites and determines which computers (not necessarily individuals) went to the sites and if the computers were compromised. A computer and possibly user name may be associated to the web site and be known by Information Security or other monitoring personnel.
2. Information Security detects activity associated with a virus or other malicious behavior. Upon identifying the computer(s) associated with the suspected activity, Information Security reviews Internet activity logs and log files on the suspected computer(s) to determine if the activity truly is malicious and a threat to University computing resources or a 'false positive'. During this review, Information Security may see websites visited, files or other information on computers, along with the computer and possibly user name associated with the suspected malicious activity.
3. IS administrators monitoring for unusual login activity identify numerous accounts being accessed from the same computer. The accounts are suspected of being compromised and immediately disabled. The accounts are re-enabled once the users contact The Bridge and change their passwords.

The people monitoring the systems may immediately disable an account in order to protect the integrity and security of the network, computers or data. If an account is disabled, then the normal procedure for re-enabling an account or addressing policy violations will be followed and the account will remain disabled until reviewed by the appropriate authority. See Section 6, Policy Violations for more details.

4. Investigations

All users will respect the user privileges of other authorized users. Individuals authorized to perform monitoring as described above will respect such user privileges consistent with their monitoring responsibilities. Thus, users will respect the rights of other users regarding security of files, confidentiality of data, and the ownership of a user's own work.

Computer and network administrators monitor and review activity in the aggregate to look for errors in functionality, usage trends, and specific suspicious or malicious activity among other details. An investigation may review specific activity of specific individuals or groups of individuals. Examples of investigations include but are not limited to:

- Review of logs to determine student activity related to assignments or grades
- Review of emails related to cheating or other honor code violations
- Review of Internet activity related to copyright violations or other potentially illegal activity
- Review of emails, computers, or Internet activity associated with reported incidents of harassment, other violations of acceptable use policies, or user complaints

Investigations are initiated at the request of only the following WFU entities:

1. Board of Trustees
2. President of the University
3. Legal Department
4. Audit and Compliance Department
5. Dean's Office(s)
6. Provost
7. Human Resources Department
8. Police Department
9. Information Security Department

All investigations require prior approvals from at least two different appropriate offices from the list above. Information from an investigation will be provided only on a need to know basis and with the approval of at least one of those who approved the investigation.

5. Prohibited Activities

The following list is intended to aid in interpreting the basic principles set out in section 2; the list should not be construed as comprehensive. Examples of actions which would be considered violations of this Policy include:

1. Copyright law violations, including but not limited to, providing copyrighted or licensed material to others while maintaining copies for one's own use, unless there is a specific provision in the license which allows this, or using a copyrighted program on more than

one machine at the same time, unless this is permitted by a specific license provision. For further information, see http://zsr.wfu.edu/scholarship/copyright/

2. Interfering with legitimate use by others of computing resources.
3. Using the computer access privileges of others.
4. Attempting to gain unauthorized access to any computer or network by hacking or malicious software.
5. Intentional downloading of malicious software or hacking tools.
6. Providing any unauthorized user with access to authorization credentials, or in any way allowing others access to a machine under one's own account. This includes providing access to campus computing resources without the express written permission of Information Systems.
7. Intentionally creating, modifying, reading or copying files (including mail) to or from any areas to which the user has not been granted access. This includes accessing, copying, or modifying the files of others without their explicit permission.
8. Disguising one's identity in any way, including sending falsified messages, and the masking of process names. This prohibition includes sending electronic mail fraudulently.
9. The establishment of any application or program which provides unauthorized access, via the Internet connection or otherwise.
10. Harassing, bullying or intimidating others, or otherwise engaging in conduct prohibited by University policies or applicable law.
11. Using University computing and/or network resources in a malicious manner including attempts to gain unauthorized access to computer systems off-campus.
12. Use of campus computer systems for commercial purposes without prior written permission of the appropriate Dean or VP, and CIO.
13. Attempting to interfere with the normal operation of computing resources in any way, or attempting to subvert the restrictions associated with such systems.
14. Attempting to circumvent data protection schemes or uncover security vulnerabilities.
15. Knowingly running or installing on any computer system or network, or giving to another user, a program to damage or place excessive load on a computer system or network.

6. Policy Violations

Suspected violation of this policy will be handled through the appropriate University process or office, such as administrative procedures, the Honor and Ethics Council, the Graduate Council, Dean's office, or Human Resources.

Violation of this policy may result in one or more of the following, in addition to any other actions deemed appropriate by the applicable authority:

1. Suspension of one's ability to perform interactive logins on relevant machines on-campus.

2. Suspension of one's ability to use the University’s computing resources.
3. Suspension of one's ability to send or receive email.
4. Increased monitoring of further computing activity (beyond normal systems monitoring).

7. Changes to This Policy

Information Security may amend this policy from time to time. Amendments must be approved through the applicable governance process and communicated to the community through an appropriate messaging system in use at that time. As with all matters of law and ethics, ignorance of the rules does not excuse violations.