CAPITAL UNIVERSITY
ACCEPTABLE USE POLICY

1.0 Overview

The computing and electronic communication resources that Capital University provides for faculty, staff, and students are essential to carrying out the University's primary mission. Protecting and preserving University computing and electronic communication resources is a cooperative effort that requires each member of the University community to act responsibly and guard against abuses.

Thousands of users share the computing resources at Capital University. These resources must be used responsibly by everyone, since misuse by even a few individuals has the potential to disrupt University business or the work of others. Users are required to exercise responsible, ethical behavior when using the University's computing resources.

Acceptable use of University computing and electronic communication resources demonstrates respect for unobstructed access, intellectual property rights including copyright, trademark, and applicable licenses, truth in communication, ownership of data, system security and integrity, and individuals' rights. Acceptable use includes, but is not limited to, respecting the rights of other users, sustaining the integrity of systems and related physical resources, and complying with all relevant policies, laws, regulations, and contractual obligations.

2.0 Purpose

The University is committed to protecting Capital University faculty, staff, students, and guests from illegal or damaging actions by individuals, either knowingly or unknowingly. The Acceptable Use Policy was written to support and protect university computing and electronic communication resources, and all users of those resources, by defining the Standards for Acceptable Use.

3.0 Scope

The scope of this policy applies to all users of Capital University computing and electronic communication resources, including faculty, staff, students, contractors, guests, individuals not otherwise affiliated with the University, and external organizations and individuals accessing external network services, such as the Internet, through University facilities.

The University's computing and electronic communication resources include its servers, network (wired and wireless) and networking facilities, e-mail system, personal computers and peripherals, software, classroom technology, multi-media equipment, websites, mobile devices and telecommunication system. These systems are the property of Capital University and are to be used for the purposes of carrying out the University's missions.

4.0 Policy

The use of the University's computing facilities in connection with University activities and minimal personal use is a privilege extended to various members in good standing of the Capital University community; it is not a right. Users of the University's computing resources are required to comply with the Acceptable Use Policy. By using these resources, all users are also subject to, and required to comply with, the User Accounts Policy, Password Policy, Information Security Policy, and other policies that apply to their specific role with the University. Users also agree to comply with all applicable federal, state, and local laws and to refrain from engaging in any activity that is inconsistent with the University's tax-exempt status or would subject the University to liability.

System Administrators and IT Support Staff must also comply with the IT Privileged Access Policy and sign the university Confidentiality Statement.

The University reserves the right to amend this Policy at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable federal, state, and local laws.

4.1 Standards of Acceptable Use

Use of University computing and electronic communication resources requires each user to adhere to the following standards of acceptable use:

- Observe all federal and state laws, as well as policies of Capital University in the use of University computing and electronic communication resources. Do not use the University’s computer resources for any unlawful purpose, such as the installation or distribution of fraudulently or illegally obtained software. The University may take any immediate steps necessary to deal with alleged violations of law or policy, including removing illegal material from the University server or other University computing or electronic communication resources.
- Respect the privacy and personal rights of others by ensuring that use of University computing and electronic communication resources does not constitute invasion of privacy, harassment, defamation, threats, intimidation, unwarranted annoyance or embarrassment, or discrimination based on race, sex, national origin, disability, age, religion, or sexual orientation.
- Respect and preserve the performance, capacity, integrity, and security of University computing and electronic communication resources. Ensure that use of those resources does not circumvent system security and does not achieve or aid others to achieve unauthorized access. The University may take any immediate steps necessary to deal with threats to performance or degradation of its computing and electronic communication resources.
- Protect the purpose of University computing and electronic communication resources to carry out the University's primary mission. Use the University’s computer resources only for the University-related purposes for which they were authorized. As with all University equipment, use of the computer resources, including the University Network, for private or commercial purposes is prohibited, except as expressly authorized. Reasonable minimal personal use is permissible within the guidelines of this policy when it does not consume a significant amount of those resources, does not interfere with the performance of the user’s job or other University responsibilities, and is otherwise in compliance with University policy. Further limits may be imposed on personal use by units or departments. Use of those resources by faculty or staff for approved consulting or other approved professional activities is not a violation of this policy.
- Respect the intellectual property rights of others by ensuring that use of University computing and electronic communication resources does not violate any copyright or trademark laws, or University licensing agreements (including licensed software).

4.2 Authorization

The University provides authorization to use University computing resources with the creation of a user account and password per the guidelines of the User Account Policy. Students, faculty, and staff obtain a user account when they register for classes or begin employment at the University.

The user account will provide access to basic computing services such as use of email, access to office automation software, the Internet, and access to systems and information that are provided based on the group the person belongs to or the position he or she holds at the University.

4.3 Appropriate Uses

Examples of computer and network uses that are encouraged, with the appropriate authorization if necessary, include, but are not limited to:

- Use of microcomputers in student labs for class assignments;
- Instructor preparation;
- Thesis research support;
- Personal computing to improve computing literacy, or to learn new computer hardware and software;
- Use of public computers for review of generally available individual or campus information;
- Use of computers provided by the university to faculty and staff in support of their work;
- Approved use of the university's information and administrative systems; and
- Use of Internet resources to promote collegial interaction and research.

4.4 Violation of Policy

Violations of acceptable use of University computing and electronic communication resources include, but are not limited to:

- Use of another person's User account
- Providing one's user account and password to someone else to use;
- Accessing or transmitting information that belongs to another user or for which no authorization has been granted;
- Any attempt to make unauthorized changes to information stored on the University's computer systems;
- Viewing data that one does not have security rights to, or should not have rights to view;
- Unauthorized copying of information stored on the University's computer systems;
- Any action that jeopardizes the availability or integrity of any University computing, communication, or information resource;
- Use of IT resources that interferes with work of other students, faculty, or staff or the normal operation of the University computing systems;

- Any attempt to bypass the University IT security systems including the Network Access Control system (NAC);
- Copying or distributing software licensed to Capital University without proper authorization;
- Stating or implying that one speaks on behalf of the University or using the University name, marks or logos without proper authorization, and not using suitable disclaimers on personal websites and other electronic communications;
- Violation of federal, state or local laws, including copyright infringement;
- Use of University-owned IT resources for personal commercial purposes; and
- Using University computing resources irresponsibly or in a way that might needlessly interfere with the work of others. This includes transmitting or making accessible offensive, annoying, or harassing material, or materials such as chain letters, unauthorized mass mailings, or unsolicited advertising; intentionally, recklessly, or negligently damaging any system, material, or information not belonging to the user; intentionally intercepting electronic communications or otherwise violating the privacy of information not belonging to or intended for the user; intentionally misusing system resources or making it possible for others to do so; or loading software or data from untrustworthy sources on to administrative systems.

5.0 Enforcement

Failure to use Capital University computing and electronic communication resources responsibly in accordance with the standards set forth in this policy threatens the atmosphere for the sharing of information, the free exchange of ideas, and the secure environment for creating and maintaining information. Any member of the University community who violates this policy may be subject to disciplinary action under appropriate University disciplinary procedures including provisions in relevant handbooks (student, faculty, administrator, and support staff).

The University may take such action as may be necessary in its discretion to address any use violation(s) under this policy, up to and including termination of a user’s account. IT may temporarily suspend or block access to an account when it reasonably appears necessary to protect the integrity, security, or functionality of computing resources, or to protect the university from liability. In addition, Capital University reserves the right to limit or restrict the use of its computing and electronic communication resources when there is evidence of a violation of applicable University policies, contractual agreements, or state or federal laws. The University may refer suspected violations of applicable law to the appropriate law enforcement agencies.

6.0 Definitions

Terms	**Definitions**
NAC	Network Access Control – NAC software tests and verifies that all computers connected to the university network have current virus protecting and operating system updates applied in order to protect the network

from spread of computer viruses, malware, and other malicious software.

7.0 Revision History

5/6/08 Draft submitted to IT Department for review.
5/27/08 Draft submitted to legal for review.
6/2/08 Comments received from legal.
6/3/08 Approved by President's Cabinet.

CAPITAL UNIVERSITY
ACCEPTABLE USE POLICY

1.0 Overview

The computing and electronic communication resources that Capital University provides for faculty, staff, and students are essential to carrying out the University's primary mission. Protecting and preserving University computing and electronic communication resources is a cooperative effort that requires each member of the University community to act responsibly and guard against abuses.

Thousands of users share the computing resources at Capital University. These resources must be used responsibly by everyone, since misuse by even a few individuals has the potential to disrupt University business or the work of others. Users are required to exercise responsible, ethical behavior when using the University's computing resources.

Acceptable use of University computing and electronic communication resources demonstrates respect for unobstructed access, intellectual property rights including copyright, trademark, and applicable licenses, truth in communication, ownership of data, system security and integrity, and individuals' rights. Acceptable use includes, but is not limited to, respecting the rights of other users, sustaining the integrity of systems and related physical resources, and complying with all relevant policies, laws, regulations, and contractual obligations.

2.0 Purpose

The University is committed to protecting Capital University faculty, staff, students, and guests from illegal or damaging actions by individuals, either knowingly or unknowingly. The Acceptable Use Policy was written to support and protect university computing and electronic communication resources, and all users of those resources, by defining the Standards for Acceptable Use.

3.0 Scope

The scope of this policy applies to all users of Capital University computing and electronic communication resources, including faculty, staff, students, contractors, guests, individuals not otherwise affiliated with the University, and external organizations and individuals accessing external network services, such as the Internet, through University facilities.

The University's computing and electronic communication resources include its servers, network (wired and wireless) and networking facilities, e-mail system, personal computers and peripherals, software, classroom technology, multi-media equipment, websites, mobile devices and telecommunication system. These systems are the property of Capital University and are to be used for the purposes of carrying out the University's missions.

4.0 Policy

The use of the University's computing facilities in connection with University activities and minimal personal use is a privilege extended to various members in good standing of the Capital University community; it is not a right. Users of the University's computing resources are required to comply with the Acceptable Use Policy. By using these resources, all users are also subject to, and required to comply with, the User Accounts Policy, Password Policy, Information Security Policy, and other policies that apply to their specific role with the University. Users also agree to comply with all applicable federal, state, and local laws and to refrain from engaging in any activity that is inconsistent with the University's tax-exempt status or would subject the University to liability.

System Administrators and IT Support Staff must also comply with the IT Privileged Access Policy and sign the university Confidentiality Statement.

The University reserves the right to amend this Policy at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable federal, state, and local laws.

4.1 Standards of Acceptable Use

Use of University computing and electronic communication resources requires each user to adhere to the following standards of acceptable use:

- Observe all federal and state laws, as well as policies of Capital University in the use of University computing and electronic communication resources. Do not use the University’s computer resources for any unlawful purpose, such as the installation or distribution of fraudulently or illegally obtained software. The University may take any immediate steps necessary to deal with alleged violations of law or policy, including removing illegal material from the University server or other University computing or electronic communication resources.
- Respect the privacy and personal rights of others by ensuring that use of University computing and electronic communication resources does not constitute invasion of privacy, harassment, defamation, threats, intimidation, unwarranted annoyance or embarrassment, or discrimination based on race, sex, national origin, disability, age, religion, or sexual orientation.
- Respect and preserve the performance, capacity, integrity, and security of University computing and electronic communication resources. Ensure that use of those resources does not circumvent system security and does not achieve or aid others to achieve unauthorized access. The University may take any immediate steps necessary to deal with threats to performance or degradation of its computing and electronic communication resources.
- Protect the purpose of University computing and electronic communication resources to carry out the University's primary mission. Use the University’s computer resources only for the University-related purposes for which they were authorized. As with all University equipment, use of the computer resources, including the University Network, for private or commercial purposes is prohibited, except as expressly authorized. Reasonable minimal personal use is permissible within the guidelines of this policy when it does not consume a significant amount of those resources, does not interfere with the performance of the user’s job or other University responsibilities, and is otherwise in compliance with University policy. Further limits may be imposed on personal use by units or departments. Use of those resources by faculty or staff for approved consulting or other approved professional activities is not a violation of this policy.
- Respect the intellectual property rights of others by ensuring that use of University computing and electronic communication resources does not violate any copyright or trademark laws, or University licensing agreements (including licensed software).

4.2 Authorization

The University provides authorization to use University computing resources with the creation of a user account and password per the guidelines of the User Account Policy. Students, faculty, and staff obtain a user account when they register for classes or begin employment at the University.

The user account will provide access to basic computing services such as use of email, access to office automation software, the Internet, and access to systems and information that are provided based on the group the person belongs to or the position he or she holds at the University.

4.3 Appropriate Uses

Examples of computer and network uses that are encouraged, with the appropriate authorization if necessary, include, but are not limited to:

- Use of microcomputers in student labs for class assignments;
- Instructor preparation;
- Thesis research support;
- Personal computing to improve computing literacy, or to learn new computer hardware and software;
- Use of public computers for review of generally available individual or campus information;
- Use of computers provided by the university to faculty and staff in support of their work;
- Approved use of the university's information and administrative systems; and
- Use of Internet resources to promote collegial interaction and research.

4.4 Violation of Policy

Violations of acceptable use of University computing and electronic communication resources include, but are not limited to:

- Use of another person’s User account
- Providing one’s user account and password to someone else to use;
- Accessing or transmitting information that belongs to another user or for which no authorization has been granted;
- Any attempt to make unauthorized changes to information stored on the University’s computer systems;
- Viewing data that one does not have security rights to, or should not have rights to view;
- Unauthorized copying of information stored on the University’s computer systems;
- Any action that jeopardizes the availability or integrity of any University computing, communication, or information resource;
- Use of IT resources that interferes with work of other students, faculty, or staff or the normal operation of the University computing systems;

- Any attempt to bypass the University IT security systems including the Network Access Control system (NAC);
- Copying or distributing software licensed to Capital University without proper authorization;
- Stating or implying that one speaks on behalf of the University or using the University name, marks or logos without proper authorization, and not using suitable disclaimers on personal websites and other electronic communications;
- Violation of federal, state or local laws, including copyright infringement;
- Use of University-owned IT resources for personal commercial purposes; and
- Using University computing resources irresponsibly or in a way that might needlessly interfere with the work of others. This includes transmitting or making accessible offensive, annoying, or harassing material, or materials such as chain letters, unauthorized mass mailings, or unsolicited advertising; intentionally, recklessly, or negligently damaging any system, material, or information not belonging to the user; intentionally intercepting electronic communications or otherwise violating the privacy of information not belonging to or intended for the user; intentionally misusing system resources or making it possible for others to do so; or loading software or data from untrustworthy sources on to administrative systems.

5.0 Enforcement

Failure to use Capital University computing and electronic communication resources responsibly in accordance with the standards set forth in this policy threatens the atmosphere for the sharing of information, the free exchange of ideas, and the secure environment for creating and maintaining information. Any member of the University community who violates this policy may be subject to disciplinary action under appropriate University disciplinary procedures including provisions in relevant handbooks (student, faculty, administrator, and support staff).

The University may take such action as may be necessary in its discretion to address any use violation(s) under this policy, up to and including termination of a user’s account. IT may temporarily suspend or block access to an account when it reasonably appears necessary to protect the integrity, security, or functionality of computing resources, or to protect the university from liability. In addition, Capital University reserves the right to limit or restrict the use of its computing and electronic communication resources when there is evidence of a violation of applicable University policies, contractual agreements, or state or federal laws. The University may refer suspected violations of applicable law to the appropriate law enforcement agencies.

6.0 Definitions

Terms	Definitions
NAC	Network Access Control – NAC software tests and verifies that all computers connected to the university network have current virus protecting and operating system updates applied in order to protect the network

from spread of computer viruses, malware, and other malicious software.

7.0 Revision History

5/6/08 Draft submitted to IT Department for review.
5/27/08 Draft submitted to legal for review.
6/2/08 Comments received from legal.
6/3/08 Approved by President’s Cabinet.