

Westminster College

Information Technology Department: Security Policy 2006-2007 Responsible Use of College Computing and Network Resources

Summary

This document covers the following:

- Terms and conditions of use of college computing and network resources;
- Appropriate and responsible use;
- Code of practice for specific activities;
- Use of electronic mail; and
- Internet access and usage.



Table of Contents

| | | |
|-----------|---|-----------|
| 1. | Introduction..... | 1 |
| 2. | Terms and Conditions of Use | 1 |
| 2.1. | User Indemnity | 2 |
| 2.2. | Limited Warranty | 2 |
| 3. | Appropriate and Responsible Use | 2 |
| 3.1. | Use of College Computing Equipment..... | 3 |
| 3.2. | Password Construction | 3 |
| 3.3. | Account Management | 4 |
| 3.4. | User Identification..... | 4 |
| 3.5. | Security..... | 4 |
| 3.6. | Confidentiality..... | 4 |
| 4. | Code of Practice for Specific Activities | 5 |
| 4.1. | Illegal Activity | 5 |
| 4.2. | Objectionable Material..... | 5 |
| 4.3. | Restricted Material | 5 |
| 4.4. | Restricted Software and Hardware..... | 5 |
| 4.5. | Copying and Copyrights..... | 6 |
| 4.6. | Sharing and Distributing Copyrighted Electronic Media | 6 |
| 4.7. | Harassment..... | 7 |
| 4.8. | Wasting Resources | 7 |
| 4.9. | Game Playing | 8 |
| 4.10. | Commercial Use | 8 |
| 4.11. | Use for Personal Business..... | 8 |
| 4.12. | Connection to the Campus-Wide Data Network..... | 8 |
| 4.13. | Printouts | 9 |
| 4.14. | Reporting Violations..... | 9 |
| 5. | Use of Electronic Mail..... | 9 |
| 5.1. | Appropriate Use of Email and User Responsibility..... | 9 |
| 5.2. | Confidentiality and Security..... | 10 |
| 5.3. | Email Deletion and Backup..... | 10 |
| 5.4. | Personal Advertising and Announcements | 11 |
| 6. | Internet Access and Usage | 11 |
| 6.1. | Online Privacy and Security Statement | 11 |
| 6.1.1. | Securing User Information | 11 |
| 6.1.2. | Use of Information | 11 |
| 6.1.3. | Use of Cookies..... | 11 |
| 6.1.4. | Student Privacy | 12 |
| 6.2. | Transmission of Information | 12 |
| 6.2.1. | Downloading | 12 |
| 6.2.2. | Suspect Information | 12 |
| 6.2.3. | Contacts | 12 |
| 6.2.4. | Information Security | 12 |
| 6.3. | Personnel Security | 12 |

| | | |
|--------|--|----|
| 6.3.1. | Resource Usage | 12 |
| 6.3.2. | Public Representations | 12 |
| 6.4. | Access Control | 13 |
| 6.5. | Reporting Security Problems | 13 |
| 6.6. | World Wide Web Publishing | 13 |
| 6.6.1. | Responsible Use..... | 13 |
| 6.6.2. | Responsibility for Web Sites and Pages | 14 |
| 6.6.3. | Official College Web Sites and Pages..... | 14 |
| 6.6.4. | Personal Web Sites and Pages..... | 14 |
| 6.6.5. | Disclaimer for Personal and Student Organization Pages | 15 |

1. Introduction

Westminster College provides its students, faculty, staff and approved guests with information technology resources facilitating education and for the institutional administration of the college. These resources include, but are not limited to, hardware, software, library and information resource databases, consulting time and expertise of staff, and Internet and network resources.

The college's computers and networks provide users with access to resources on- and off-campus and give them the ability to communicate with others worldwide. This access requires users to act responsibly and adhere to legal and ethical standards. Users should be considerate of the needs of others, do nothing to impede anyone else's ability to use the computer and network resources, and observe all relevant laws and regulations.

Any user of college computing equipment or resources is deemed to have understood and accepted all current policies. Users are expected to follow the standards and guidelines of this policy. Failure to comply with the standards and guidelines for responsible use will result in disciplinary action. Serious or multiple infractions may cause the user to be denied access to college computers and networks. It is the responsibility of each individual to be familiar with and abide by all current policies.

2. Terms and Conditions of Use

The following list, though not covering every situation, specifies some of the terms and conditions for use of Westminster College's computing and network resources:

1. The college reserves the right to limit, restrict, or extend access to computing and network resources.
2. Those using the computing and network resources are responsible for the appropriate use of the resources provided as detailed in this policy.
3. College computing and network resources are only to be used by authorized personnel for non-commercial purposes. Commercial, for-profit activities are prohibited, unless officially sanctioned by the college.
4. The college endeavors to protect the confidentiality of information and material furnished by the user and instructs all computing personnel to protect the confidentiality of such information and material.
5. The college endeavors to safeguard the possibility of loss of information within the college's computing and network resources but is not liable to the user in the event of any such loss. The user must take all reasonable measures to further safeguard against any loss of information within the college's computing and network resources.
6. When users of the computing and network resources cease to be formally associated with the college (e.g. no longer an employee, enrolled student, or visitor to the college), their information may be removed from college computing and network resources without notice. Users must remove their information or make arrangements for its retention prior to leaving the college.
7. The college reserves the right to limit permanently or restrict any user's usage of the computing and network resources; to copy, remove, or otherwise alter any information or system that may undermine the authorized use of the computing and network resources; and

to do so with or without notice to the user in order to protect the integrity of the computing and network resources against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

8. The college, through authorized individuals, reserves the right to periodically check and monitor the computing and network resources, and reserves any other rights necessary to protect them.
9. The college reserves the right to take emergency action to safeguard the integrity and security of the computing and network resources. This includes but is not limited to the termination of a program, job, or on-line session, or the temporary alteration of user account names and passwords.
10. The college disclaims any responsibility and/or warranties for information and materials residing on non-college computer systems or available over publicly accessible networks, except where such responsibility is formally expressed. Such materials do not necessarily reflect the attitudes, opinions, or values of Westminster College, its staff, or students.
11. Information published on Westminster's web site is expected to be in compliance with laws that govern electronic media with regard to copyrighted material, confidential information and libelous remarks and with other applicable laws and college policies. The opinions, interest and activities expressed on student, staff and faculty personal pages are strictly those of the page author. Individuals who maintain personal web sites or pages assume responsibility and liability for the content of their documents. The contents of personal web sites or pages have not been reviewed or approved by Westminster College.
12. Direct connectivity to the Internet to individuals and organizations outside of the college is prohibited without the explicit permission of the Westminster College Information Technology department.

2.1. User Indemnity

Users agree to indemnify the college for any loss or damage arising out of improper use.

2.2. Limited Warranty

The college takes no responsibility for and provides no warranty against the non-delivery or loss of any files, messages or data, nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

3. Appropriate and Responsible Use

Appropriate and responsible use of the Westminster computing and network resources is defined as use that is consistent with the teaching, learning, research, and administrative objectives of the college. None of these policies are meant to inhibit academic pursuits or academic freedom. As long as the activity is a legitimate academic pursuit, not illegal, is not clearly and expressly prohibited, and does not damage computing and network resources, this policy does not prohibit the academic activity.

Users of the Westminster computing and network resources accept the following specific responsibilities:

- To not create, display or transmit threatening, racist, sexist, obscene, abusive, or harassing

language or materials. Westminster college is committed to being a racially, ethnically, and religiously heterogeneous community.

- To uphold local, state, or federal laws; copyright laws; or institutional rules.
- To use only authorized computer accounts and passwords.
- To not use email or other electronic communications technologies to harass or threaten others; for promotional, profit-making purposes; or to break into or read others' email or electronic correspondence without their permission.
- To respect the integrity of the computing and network resources by not doing intentional damage to hardware, software, security devices or code, or through the creation of viruses, worms, Trojans or other forms of electronic mayhem.
- To not seek unauthorized access to computers at other locations.
- To not use the computing and network resources in a way that inhibits the normal academic and administrative activities of the college.

3.1. Use of College Computing Equipment

All faculty, staff, and students are required to store all official college data (academic, scholastic, and research work; official electronic information and work data files, etc.) on specifically designated network storage locations which are supported and backed-up by the Information Technology department.

Users are responsible for the security and integrity of college information while using college computer and network resources. User responsibility includes controlling physical and network access to workstations. Users may not store or share college passwords or other information that can be used to gain access to other campus computing resources. Users may not store college passwords or any other confidential data or information on their personal computing equipment or digital media (disks, memory cards, etc.).

The Information Technology department is responsible only for standard college software and hardware on college-owned computers (either desktop or portable), servers, and the computing network and is not responsible for recovering data stored on local workstations or personal computing devices. Users are responsible for any additional hardware they attach, software they install, or data they store on workstation(s). In cases of workstation hardware or software problems, Information Technology will "reimage" the workstation, overwriting anything on the local workstation hard drive(s), and/or replace hardware as needed. Information Technology also reimages all workstations at least once per year as part of workstation maintenance.

3.2. Password Construction

Users are instructed not to share their Westminster computer user account password(s) with anyone. Information Technology department staff will never ask for passwords.

Passwords must adhere to the following:

- Passwords must be at least five characters long with no spaces or quotes.
- Passwords should not use birthdates, phone numbers, family or pet names, or any part of the username.

- A password should not be a word from the dictionary. Most basic cracking programs contain over 80,000 words, and plenty of variations.

The strongest passwords use a combination of MiXed caSe letters, numbers, and symbols. For example:

- T@nsTa@fL! (There ain't no such thing as a free lunch!)
- Iam#3oF5 (I am the third of five children)

3.3. Account Management

- A network account is provided by the college in the individual user's name for their use only.
- Users may not share accounts with or make passwords available to any other person.
- Users may not use the account of any other person.
- Faculty, staff, and students are required to change passwords immediately upon receipt of an account.
- Faculty and staff are required to change their passwords every 120 days. Students are encouraged to change their accounts at least every 120 days.

3.4. User Identification

Campus computing resources are provided for Westminster faculty, staff, and students only. Users must carry a college Photo ID at all times while using campus computing resources. Security, Information Technology, and Lab Help Desk staff may deny access to computing resources to anyone without proper identification.

3.5. Security

Users of the Westminster computing and network resources accept the following specific responsibilities:

- To safeguard their data, personal information, passwords and authorization codes, and confidential data;
- To take full advantage of file security mechanisms built into the computing systems;
- To choose their passwords wisely and to change them periodically;
- To follow the security policies and procedures established to control access to and use of administrative data.

3.6. Confidentiality

Users of the Westminster computing and network resources accept the following specific responsibilities:

- To respect the privacy of other users; for example, not to intentionally seek information on, obtain copies of, or modify files, tapes, data, or passwords belonging to other users or the college;
- Not to represent others, unless authorized to do so explicitly by those users;

- Not to divulge sensitive personal data to which they have access concerning staff or students without explicit authorization to do so.

4. Code of Practice for Specific Activities

4.1. Illegal Activity

Using or giving access to information on the college computing and network resources that could result in legal action against the college constitutes inappropriate use.

4.2. Objectionable Material

The college's computing and network resources may not be used for the transmission, obtaining possession, demonstration, advertisement, or requesting the transmission of the following types of material:

1. Child pornography;
2. Material that promotes crime or violence, or incites or instructs in matters of crime or violence; or
3. Material that describes or depicts in a manner that is likely to cause offence to a reasonable adult. For example:
 - The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct;
 - Sexual conduct with or upon the body of a dead person;
 - The use of urine or excrement in association with degrading or dehumanizing conduct or sexual conduct;
 - Bestiality;
 - Acts of torture or the infliction of extreme violence or extreme cruelty.

4.3. Restricted Material

The college's computing and network resources may not be used to transmit restricted material to a minor. Restricted material is defined as material that relates to matters of sex, drug misuse, crime, cruelty, violence, or revolting or abhorrent phenomena that a normal adult would regard as unsuitable for a minor to see, read, or hear.

4.4. Restricted Software and Hardware

Users should not knowingly possess, give to another person, install on any of the computing and network resources, or run programs or other information which could result in the violation of any college policy or the violation of any applicable license or contract. This is directed towards but not limited to software known as viruses, Trojan horses, worms, password breakers, and packet observers. Authorization to possess and use viruses, Trojan horses, worms, password breakers, and packet observers for legitimate research or diagnostic purposes must be obtained from the Information Technology department.

The unauthorized physical connection of monitoring devices to the computing and network

resources which could result in the violation of college policy or applicable licenses or contracts is inappropriate use. This includes but is not limited to the attachment of any electronic device to the computing and network resources for the purpose of monitoring data, packets, signals, or other information. Authorization to possess and use such hardware for legitimate diagnostic purposes must be obtained from the Information Technology department.

4.5. Copying and Copyrights

Users of the computing and network resources must abide by the Westminster College Copyright Policy, which covers copyright issues pertaining to college faculty, staff and students.

Respect for intellectual labor and creativity is essential to academic discourse. This tenet applies to works of all authors and publishers in all media. It includes respect for the right to acknowledgment and right to determine the form, manner, and terms of publication and distribution. If copyright exists, as in most situations, it includes the right to determine whether the work may be reproduced at all. Because electronic information is volatile and easily reproduced or altered, respect for the work and personal expression of others is especially critical in computing and network environments. Viewing, listening to, or using another person's information without authorization is inappropriate use of the resources. Standards of practice apply even when this information is left unprotected.

Most software that resides on the computing and network resources is owned by the college or third parties and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the computing and network resources or for distribution outside the college; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain; and against public disclosure of information about programs (e.g., source code) without the owner's authorization.

With a greater emphasis on computer-based assignments, students need to be especially cognizant of the appropriate use of computing and network resources. In particular, academic dishonesty or plagiarism in a student assignment may be suspected if the assignment calling for independent work results in two or more solutions so similar that one can be converted to another by a mechanical transformation. Academic dishonesty in an assignment may also be suspected if a student who was to complete an assignment independently cannot explain both the intricacies of the solution and the techniques used to generate that solution. Suspected occurrences of academic dishonesty are referred to the dean of the school.

4.6. Sharing and Distributing Copyrighted Electronic Media

It is a violation of federal law and Westminster policy to share and/or distribute copyrighted materials without the permission of the copyright holder. Violators may be subject to civil and criminal prosecution under the provisions of the Digital Millennium Copyright Act (DMCA) and may also be subject to personal sanctions by the college.

Popular file sharing programs commonly share files from computers after users have installed them. Many users do not realize that this software may turn their personal computer into a server, or upload site, even if that was not their intention. Files on a network-connected PC may then be illegally shared with every other person connected to the World Wide Web. It is imperative that

users disable the file sharing capability of these systems. Users who do not know how to disable such file sharing capability should contact the Information Technology department.

Industry representatives aggressively monitor the Internet to discover incidents of illegal file sharing of music, games or video. When violations are discovered, they contact the network owner and/or the Internet Service Provider and demand that the offending device be disconnected from the network. To protect the user and the college from culpability under the DMCA or college policy, the college will disable network access for any machine for which a DMCA complaint has been received.

To restore network service, the user must contact the Dean of Students and arrange to sign a document stating that the user has disabled the file sharing function of the software and has agreed to discontinue all illegal file sharing activity. Action taken by the college to remedy a violation does not preclude the copyright holder from seeking civil and/or criminal prosecution.

4.7. Harassment

College policy prohibits sexual and discriminatory harassment. Westminster's computing and network resources are not to be used to libel, slander, or harass any other person.

The following constitute examples of computer harassment:

1. Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;
2. Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
3. Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection);
4. Intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another;
5. Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

The display of offensive material in any publicly accessible area is likely to violate college harassment policy. Materials are available on the Internet and elsewhere that some members of the college community will find offensive. One example is sexually explicit graphics. The college does not restrict the availability of such material, but it considers its display in a publicly accessible area to be inappropriate. Public display includes, but is not limited to, publicly accessible computer screens and printers.

4.8. Wasting Resources

Deliberately performing any act that impairs the operation of any part of the computing and network resources or denies access by legitimate users to any part of them constitutes inappropriate use. This includes but is not limited to wasting resources, tampering with components, or reducing

the operational readiness of the resources.

The willful wasting of computing and network resources is inappropriate use. Wastefulness includes but is not limited to passing chain letters, willful generation of large volumes of unnecessary printed output or disk space, willful creation of unnecessary multiple jobs or processes, or willful creation of heavy network traffic. In particular, the practice of willfully using the college's computing and network resources for the establishment of frivolous and unnecessary chains of communication connections is an inappropriate waste of resources.

The sending of random mailings ("junk email" or "spam") is inappropriate use. The Information Technology department has specific distribution lists for conveying official college information via email; users may not opt out of these lists. In addition, the department has set up other general communication lists which users may opt out of. Users wishing to send mass emails should contact Information Technology to discuss appropriate usage and options for distribution.

4.9. Game Playing

Limited recreational game playing that is not part of an authorized and assigned research or instructional activity is permitted as long it does not interfere with the academic or administrative functioning of computing and network resources. College computing and network services are not to be used for extensive or competitive recreational game playing. Recreational game players occupying a seat in a public computing facility may not in any way interfere with other users' computing needs and must give up that computing position when others who need to use the facility for academic or research purposes are waiting.

4.10. Commercial Use

College computing and network resources are provided by the college for the support of its mission. It is inappropriate to use the computing and network resources for:

1. Commercial gain or placing a third party in a position of commercial advantage.
2. Non-college related activity.
3. Commercial advertising or sponsorship except where such advertising or sponsorship is clearly related to or supports the mission of the college or the service being provided.

This standard is not intended to restrict free speech or to restrict the college from setting up information servers or other services specifically designated for the purpose of fostering an "electronic community" with the wider community the college serves.

4.11. Use for Personal Business

The college's computing and network resources may not be used in connection with compensated outside work or for the benefit of organizations not related to Westminster College, except in connection with scholarly pursuits such as academic publishing activities or sanctioned faculty consulting. This and any other incidental use such as electronic communications or storing data on single-user machines must not interfere with other users' access to resources (network bandwidth, disk space, printers, etc.) and must not be excessive.

4.12. Connection to the Campus-Wide Data Network

Most campus buildings are included in the campus network. To maintain the integrity of the college computing and network resources, connections to the campus network are made only by specialized

personnel under the direction of Information Technology. Users may attach appropriate equipment such as personal computers, laptops, personal data assistants, game consoles, and other end-user devices only at existing user-connection points. Users may not attach network related hardware such as routers, switches, hubs, wireless access points, etc., or share their Internet connection. All requests for additional network connections or for the relocation of a connection should be directed to the Information Technology department.

Users connecting to the Westminster network should be aware that there is no assumption of privacy. In order to protect users and service business and academic needs, any and all network traffic may be inspected and monitored by authorized Information Technology personnel.

4.13. Printouts

Users are responsible for the security and privacy of printouts of college information.

4.14. Reporting Violations

Users of the Westminster computing and network resources accept the responsibility to report any information concerning instances in which the college Information Technology Security Policy or any of its standards and codes of practice has been or is being violated.

Reports about violations should be sent to the Director of Information Technology as well as the Information Technology staff member(s) acting as custodian(s) of the system where the violation occurred.

5. Use of Electronic Mail

Electronic mail (“email”) and communications resources provided by Westminster College are intended for teaching, research, outreach, and administrative purposes. Their use is governed by college rules and policies, applicable laws, and acceptable use policies. Electronic mail may be used for personal communications within appropriate limits.

These standards of use cover all electronic mail systems used by members of the college community from the college’s network or connecting to the college’s network or while users are acting in official college capacities.

5.1. Appropriate Use of Email and User Responsibility

Email can be both informal like a phone call and yet irrevocable like an official memorandum. Because of this, users should explicitly recognize their responsibility for the content, dissemination, and management of the messages they send.

This responsibility means ensuring that messages:

- Do not contain information that is harmful to the college or members of the college community;
- Are courteous and polite;
- Are consistent with college policies;
- Protect others’ right to privacy and confidentiality;
- Do not contain obscene, offensive, or slanderous material;

- Are not used for purposes that conflict with the college’s interests;
- Do not unnecessarily or frivolously overload the email system (e.g., spamming and junk mail are not allowed);
- Are not for commercial purposes unless authorized by the college.

5.2. Confidentiality and Security

All users of the Westminster email system should be aware that:

- Email is inherently not a secure technology.
- The college retains the right to allow authorized college officers to monitor and examine the information stored within the college network and computers.
- Personal confidential material should not be stored on or sent through college equipment.
- Sensitive or confidential college information should not be sent through the electronic mail system unless it is encrypted.
- Users must ensure the integrity of their password and abide by college policy on password security.
- Users must assess each email individually to decide if it is legitimate and cannot rely on the displayed sender address, which are easy to fake. If in doubt of the authenticity of an email, users are instructed to call the author and verify it.
- Users should not respond to emails asking them to provide confidential information (usually by following a hyperlink to a web page with a form, or by filling out a form in the email).
- Users should assume every email attachment contains malicious software and scan all attachments with virus detection software prior to opening the file(s).
- Users should not reply to or follow “unsubscribe” links in suspicious emails.
- Users should use the email system’s Junk Mail handling tools to block spam and unwanted email. Spam should be forwarded as an attachment to stopspam@westminstercollege.edu.

5.3. Email Deletion and Backup

The Information Technology department performs holistic data backups on the official college email system in order to restore email services in the event of a critical emergency, such as an event requiring implementation of a disaster recovery plan.

All users of the Westminster email system should be aware that:

- To protect user privacy, individual emails can not be restored. Users deleting email do so with the understanding that it is a permanent, irrevocable action.
- It is the responsibility of users to archive email they wish to permanently save. Archived email is not automatically deleted and is backed up regularly.
- Sent email delivered to another account within the college’s email system is automatically deleted after 15 days if it has not been opened.

- Sent email delivered to another account within the college's email system is automatically deleted after 120 days after it has been opened.
- Email moved to the email system trash is automatically deleted every 7 days.

5.4. Personal Advertising and Announcements

College email is not to be used for personal advertising or announcements.

6. Internet Access and Usage

The resources, services, and inter-connectivity available via the Internet introduce new opportunities and new risks. In response to the risks, this statement describes Westminster College's official policy regarding Internet security. It applies to all college employees, students, contractors, and temporaries who use the Internet with college computing or network resources, as well as those who represent themselves as being connected with Westminster College.

6.1. Online Privacy and Security Statement

Westminster College handles user-provided information with the utmost of respect and care. This statement describes what Westminster does to secure user-provided information and how such information is used.

6.1.1. Securing User Information

Westminster uses a number of standard technologies and procedures for security. These include but are not limited to:

- Encryption. Westminster use Secure Sockets Layer (SSL) encryption to protect information during transmission.
- Network Privacy and Restriction. Westminster uses a variety of secure firewalls to control access to data.
- Passwords and User Accounts. Westminster allows access to college data only to authorized personnel.
- Access Exclusion. Westminster uses Internet Protocol (IP) restriction to increase security, where appropriate.
- Continual Session States (timeouts). Westminster uses session states to increase security, where appropriate.

6.1.2. Use of Information

Westminster maintains user-provided information as part of the college database. This information is used for the purpose of communicating by mail, telephone, and email and other electronic communication technologies. Westminster does not sell lists and does not provide information to third parties that are not affiliated with the college.

6.1.3. Use of Cookies

Cookies are small files used as identifiers on the Internet. Cookies are transferred to users' computers through web browsers. Westminster uses cookies to track traffic to the official college

website and for a variety of useful Internet applications. While users can disable cookies in their web browsers, Westminster recommends users allow cookies in order to best experience the college web site and much of the Internet.

6.1.4. Student Privacy

The college follows federal guidelines (FERPA) for information related to currently enrolled students.

6.2. Transmission of Information

6.2.1. Downloading

All software downloaded from non-college sources via the Internet must be screened with virus detection software prior to being run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone, non-networked machine.

6.2.2. Suspect Information

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. No quality control process exists on the Internet, and a considerable amount of information from the Internet is outdated or inaccurate.

6.2.3. Contacts

Contacts made over the Internet should not be trusted with college information unless reasonable steps have been taken to ensure the legitimacy of the contacts. This applies to the release of any internal college information.

6.2.4. Information Security

Wiretapping and message interception is straightforward and frequently encountered on the Internet. Accordingly, college, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Credit card numbers, log-in passwords, and other parameters that can be used to gain access to college systems, networks and services, must not be sent over the Internet in readable form.

6.3. Personnel Security

6.3.1. Resource Usage

Westminster College encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not college time. Likewise, games, newsgroups, and other non-college activities must be performed on personal, not college time. Use of college computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no college activity is pre-empted by personal use.

6.3.2. Public Representations

Users may indicate their affiliation with the college in bulletin board discussions and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an email address. In either case, whenever users provide an affiliation, they must also clearly indicate the opinions expressed are their own or not necessarily those of Westminster College. To avoid libel problems, whenever any affiliation with the college is included with an

Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

All users must not publicly disclose internal college information via the Internet that may adversely affect the college's relations or public image. Care must be taken to properly structure comments and questions posted to mailing lists, public newsgroups, and related public postings on the Internet.

6.4. Access Control

Unless the prior approval of the Director of Information Technology has been obtained, faculty, staff, and students may not establish modems, Internet, or other external network connections that could allow non-college users to gain access to college systems and/or networks and college information.

Likewise, unless the Director of Information Technology has provided approval in advance, users are prohibited from using new or existing Internet connections to establish new communication channels. These channels include but are not limited to electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, and on-line database services.

6.5. Reporting Security Problems

The Information Technology department must be notified immediately when:

- Sensitive college information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
- Unauthorized use of college information systems has taken place, or is suspected of taking place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- There is any unusual systems behaviour, such as missing files, frequent system crashes, or misrouted messages.

Security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users other than specific Information Technology department staff must not attempt to probe computer security mechanisms at Westminster College or other Internet sites, and doing so is considered inappropriate use.

6.6. World Wide Web Publishing

Westminster College recognizes the educational value and potential of publishing on the World Wide Web and encourages students, staff and faculty to publish electronic information. The college also recognizes that the quality of the information Westminster College presents on its web site plays an important role in fostering and maintaining the college's reputation and image. The policy and guidelines described in this statement seek to ensure that the material published on the web site reflects Westminster's educational purpose and adheres to college standards that result in electronically published information that is visually appealing, accurate, and well written.

6.6.1. Responsible Use

Those who publish information on Westminster's web site are expected to comply with Federal,

state and local laws governing electronic media, including copyrighted material, photographic images, sound prints, confidential information, and libellous remarks. If applicable laws or Westminster policy are violated or disregarded, the college reserves the right to suspend publishing privileges or remove pages.

6.6.2. Responsibility for Web Sites and Pages

The rate of growth and change in the Westminster web site necessitates a distributed web site content management system and precludes any systematic review of published material by a single individual or group. College administrative units, groups, and individuals trained by the Information Technology department have the responsibility for creating and maintaining specific content on the official web site. The Information Technology web team, Office of Admissions, and the Office of Communications reserve the right to edit, modify, add, and delete any and all content and media on the official college web site as needed without notice.

Two broad categories of web pages exist: official college pages and personal pages.

6.6.3. Official College Web Sites and Pages

Official college web sites and pages are created and maintained by trained content contributors under the direction of the Information Technology staff and in accordance with college web guidelines and conventions. Official web sites and pages support the educational mission of the college and include such material as the campus calendar, course schedules, course syllabi, job announcements, departmental and academic sites, marketing materials, electronic services, and general college information.

Each content contributor is responsible for ensuring that the electronic information they oversee is accurate and up to date. Official sites and pages are reviewed once yearly and as needed by the Westminster Web Content Committee.

6.6.4. Personal Web Sites and Pages

As a service to the Westminster community, and to encourage use of technology as a tool for teaching and learning, the Information Technology department provides personal web space for faculty, staff, and students. Note that the college is not an Internet Service Provider and makes no guarantees as to the availability or accessibility of hosted personal web sites or any other electronic media. No guarantee of services or support beyond data backup associated with the individual user account is made or implied.

Personal web sites and pages are those created and maintained by individual faculty, staff, or students and hosted on Westminster web servers. Personal web sites and pages are the property and responsibility of the person to whom the account is assigned. Individuals may not use these web sites and pages for personal business or personal gain unless approved by the college, and all hosted personal pages and sites must adhere to the policies set forth in this document.

Faculty, staff, and students choosing to put personal web sites, pages, or any other electronic media online do so with the explicit understanding that the information is publicly accessible and will be found, categorized, and linked to by a wide variety of Internet search engines within hours of being posted.

Personal web sites and pages should include the following elements:

- Name and email of the owner;

- Date of the last update;
- Disclaimer.

6.6.5. Disclaimer for Personal and Student Organization Pages

All faculty, staff, and student personal pages and student organization pages are bound by and must include the following disclaimer:

"The opinions, interests, and activities expressed on this page are strictly those of the page author. Individuals who maintain personal pages assume responsibility and liability for the content of their documents. The contents of this page have not been reviewed or approved by Westminster College."