

College of DuPage

Information Technology

Electronic Communications Guidelines

9/9/2009

TABLE OF CONTENTS

1.0 PURPOSE AND SCOPE.....	4
1.1 OVERVIEW	4
1.2 SCOPE	4
1.2.1 <i>Foundation and Legal Background</i>	4
1.2.2 <i>Access and Use</i>	4
1.2.3 <i>Privacy</i>	4
1.2.4 <i>Security, Records, and Archiving</i>	4
2.0 FOUNDATION & LEGAL BACKGROUND.....	5
2.1 INTRODUCTION	5
2.2 DEFINITIONS	5
2.3 RESPONSIBILITIES	5
2.4 LAW	5
3.0 ACCESS AND USE	6
3.1 INTRODUCTION	6
3.2 AUTHORIZATION	6
3.3 PROPERTY RIGHTS	6
3.4 ALLOWABLE USERS	7
3.4.1 <i>Terms of Allowable Use</i>	7
3.4.2 <i>Purposes</i>	7
3.5 RESTRICTIONS.....	7
3.5.1 <i>Unlawful Activities</i>	7
3.5.2 <i>Business Enterprises</i>	7
3.5.3 <i>Endorsements and Promotions</i>	7
3.5.4 <i>Personal Financial Gain</i>	8
3.5.5 <i>Capacity Overload</i>	8
3.5.6 <i>College Policies</i>	8
3.5.7 <i>Other</i>	8
3.6 DISCLAIMERS.....	8
3.6.1 <i>Sample Disclaimer</i>	8
3.7 FALSE IDENTITIES	8
3.8 PERSONAL USE	9
3.8.1 <i>Interfere with College Electronic Communications Facilities</i>	9
3.8.2 <i>Incur Costs</i>	9
3.8.3 <i>Compromise the College Mission</i>	9
3.8.4 <i>Clash with Job Duties</i>	9
3.9 UNSOLICITED COMMUNICATION	9
3.10 ACCESSIBILITY.....	9
3.11 INTELLECTUAL PROPERTY.....	9
3.12 E-MAIL	10
3.12.1 <i>Unauthorized E-Mail Practices</i>	10
3.13 eBOARD – ELECTRONIC BULLETIN BOARD	11
3.14 PUBLIC AND SHARED FOLDERS	11
3.15 NETWORK STORAGE FOR DEPARTMENT AND INDIVIDUAL USE.....	11
3.16 DISTRIBUTION	11
3.17 APPROVAL AND AUTHORIZATION	11
3.18 RESPONSIBLE PERSON.....	12
3.19 WEB PAGES.....	12
3.19.1 <i>Identification</i>	12
3.19.2 <i>Official Web Pages</i>	12
3.19.3 <i>Individual Web Pages</i>	12
3.20 COURSE MANAGEMENT SYSTEM(S).....	12

3.21 VOICE SYSTEMS.....	13
3.22 BROADCAST RADIO AND TELEVISION	13
3.22.1 Licensing.....	13
3.22.2 Broadcast Interference.....	13
3.22.3 Broadcast Content.....	13
3.23 CABLE TELEVISION.....	13
3.24 STREAMING AUDIO AND VIDEO	13
3.25 OTHER WIRELESS DEVICES.....	14
3.26 PENALTIES	14
4.0 PRIVACY.....	15
4.1 INTRODUCTION	15
4.2 EXCEPTIONS TO PRIVACY STANDARDS	15
4.2.1 Protected Information.....	15
4.2.2 Other Limits on Privacy.....	15
4.3 USER RESPONSIBILITIES.....	16
4.4 ACCESS WITHOUT CONSENT.....	18
4.4.1 Exceptions.....	18
4.4.2 Authorization.....	18
4.4.3 Guidelines.....	19
4.4.4 Emergencies.....	19
4.4.5 Notification.....	19
4.4.6 Compliance with Law.....	19
5.0 SECURITY, RECORDS, AND ARCHIVING	20
5.1 INTRODUCTION	20
5.2 USER RESPONSIBILITY	20
5.3 ACCESS	20
5.4 SECURITY BREACHES.....	20
5.5 RECORDS AND ARCHIVING.....	20
6.0 USES	21
6.1 EMPLOYEE TRAINING	21
7.0 APPENDIX: DEFINITIONS.....	22
ACCESS/USE.....	22
COLLEGE ELECTRONIC COMMUNICATIONS RECORD	22
COLLEGE ELECTRONIC COMMUNICATIONS SYSTEMS OR SERVICES	22
COLLEGE RECORD.....	22
COMPELLING CIRCUMSTANCES	22
ELECTRONIC COMMUNICATIONS	23
ELECTRONIC COMMUNICATIONS FACILITIES	23
ELECTRONIC COMMUNICATIONS RECORDS	23
ELECTRONIC COMMUNICATIONS SYSTEMS OR SERVICES	23
EMERGENCY CIRCUMSTANCES	23
HOLDER OF AN ELECTRONIC COMMUNICATIONS RECORD OR ELECTRONIC COMMUNICATIONS HOLDER	23
OFFICIAL COMMUNICATIONS.....	23
POSSESSION OF ELECTRONIC COMMUNICATIONS RECORD	23
SUBSTANTIATED REASON.....	24
TIME-DEPENDENT, CRITICAL OPERATIONAL CIRCUMSTANCES.....	24
USER OF ELECTRONIC COMMUNICATIONS SERVICES.....	24
WEB PORTAL SYSTEM.....	24
WEB-BASED SYSTEM.....	24

1.0 Purpose and Scope

1.1 Overview

Comprehensive electronic communications guidelines are essential to define the appropriate access, use, privacy, security, responsibilities, and limitations in the use of electronic communications at the College. The College provides interactive and one-way electronics services that include, but are not limited to, voice telephone, voice mail, FAX services, teleconferencing, video conferencing, electronic mail, electronic bulletin boards, list-servers, newsgroups, Internet access, web pages, traditional print information published electronically, licensed software, licensed computer systems, and electronic broadcasting in radio and television.

1.2 Scope

These guidelines will cover four major topics:

1.2.1 Foundation and Legal Background

Define the foundation and the legal background of the electronic communications guidelines. This includes the employee and student responsibilities for understanding these guidelines and that these guidelines are defined by public law and policies.

1.2.2 Access and Use

Accessibility is defined, in addition to appropriate use of electronic communications, by College faculty, students, staff, and the College community.

1.2.3 Privacy

Privacy addresses institutional and user expectations of privacy and standards for maintaining privacy that are consonant with the public law, the body of College policies, community values, and realistic expectations of technological capability.

1.2.4 Security, Records, and Archiving

Security defines the parameters by which electronic communications are kept secure, both through technology and organizational governance as defined by College policies, public law, record keeping, archival needs, technology resources, and staff capabilities.

2.0 Foundation & Legal Background

2.1 Introduction

This section defines all essential terms, delineates major responsibilities for electronic communications, and spells out the fundamental guidelines.

2.2 Definitions

The meanings of essential terms used throughout this document are contained in 7.0, Appendix: Definitions.

2.3 Responsibilities

The Vice President of Information Technology is responsible for the development and revision of *Electronic Communications Guidelines*.

Each employee is responsible for understanding Board policy and the *Electronic Communications Guidelines* as it applies to their job. They are also responsible to see that their students, administrative units, members of the public, and employees know, understand, and follow them. The College will provide biannual training on policy and guidelines for employees.

2.4 Law

Both public law and policies prohibit the theft or abuse of all its computers, other electronic software and support systems, including computers that support electronic communications facilities, systems, and services. Electronic communications facilities include voice systems, broadcast facilities, cable television, and College computing facilities including, but not limited to, the mainframe computer, servers, the entire network system/infrastructure, desktops, laptops, and other devices such as palmtops.

Abuses include, but are not limited to, unauthorized entry, use, transfer, tampering with the communications, and/or work of others and with other electronic communications facilities, systems, and services. Certain types of abuses constitute criminal behavior. All employees are encouraged to familiarize themselves with these laws and their relation to College policies and guidelines. For example, the Patriot Act and the Children's Internet Protection Act could have significant consequences for College electronic communications and access to them.

In addition to legal sanctions, violators of these guidelines may be subject to disciplinary action including dismissal or expulsion, as relevant, consistent with other College policies, procedures, or collective bargaining agreements.

3.0 Access and Use

3.1 Introduction

The College has made a significant investment in electronic communications technologies to increase capacity to accommodate more users and more applications and to provide higher quality service. These investments are intended to improve College instruction, instructional support for its students, and professional and management support for all employees through use of electronic communications. Nonetheless, like books in a library or classroom space, there are restrictions that insure sensible use of the facilities to enable them to be used effectively and efficiently. Reliable operation, privacy, security, and fair access are the goals. Should the College deem it necessary, it reserves the right to control usage through denying or restricting access to these facilities.

3.2 Authorization

There are levels of access and authorizations required for use of the College electronic communications systems. Some require the completion of account request forms and authorization by the supervisor. Use of specific electronic communications systems may be a necessary condition for employment. The new employee orientation process and on-going training will give the basic parameters for these authorizations.

3.3 Property Rights

College electronic communications systems and services are College facilities. All electronic communications addresses, sites, numbers, accounts, and other identifiers associated with the College or any College unit, or assigned by the College to individual or other organizations are the property of the College unless these are considered private correspondence.

Likewise, electronic communications records pertaining to the business of the College are College records, whether or not the College owns the electronic communications facilities, systems, or services used to create, send, forward, reply to, transmit, store, hold copy, download, display, view, read, print, or otherwise record them.

Clearly there are exceptions in the matter of ownership of communication content, (e. g., work that is under copyright not owned by the College or otherwise defined by public law or by other College policies). Nonetheless, the College underscores that, given these conditions of ownership; staff should use the College systems with care and exercise similar restraints and cautions to those exercised over the other forms of communication or more tangible forms of College property. No less care should apply to the property of others on College premises.

The college reserves the right to access and examine the files and/or actual network activity of any College IT infrastructure user to investigate violations or suspected violations of security and/or college policy, or network interactions which may be contributing to poor computing equipment performance or computing equipment malfunctions pursuant to section 4.2 and section 4.4 below. For this reason, users must regard themselves as having no expectation of ownership or privacy with regard to their files, data, or communications while using the college IT infrastructure.

3.4 Allowable Users

College faculty, staff, students, members of the public and others affiliated with the College (including those in program, contract, or license relationships) may use College electronic communications facilities and services for purposes defined under Allowable Use. Members of the public also may use these facilities under the caveats specified under Terms of Allowable Use. The College will determine specific guidelines to enable allowable users to access its systems. Changes in status of current users including, but not limited to, termination, retirement, resignation, academic dismissal, disciplinary dismissal, voluntary ending of student status, and freezing of records will also end access to all College computer assets and electronic communications facilities including, but not limited to, voice telephone services, e-mail, web pages, computer sign-ons, and access to College records. Exceptions to these requirements must be in writing and/or in conformance to other Board policies.

3.4.1 Terms of Allowable Use

Those who use College electronic communication facilities must do so responsibly; i. e., comply with the public law, all College policies and guidelines, and reasonable standards of professional and personal courtesy and conduct. All electronic communications are governed by College policies (unless specifically excluded by these policies) that govern use of College facilities. The following set out the terms of allowable use.

3.4.2 Purposes

College electronic facilities are primarily for the use of instruction, instructional support, and public service. No outside agencies or individuals may use College electronic communications facilities unless their services support the College and its mission. Exceptions will require permission in writing by responsible College authorities.

3.5 Restrictions

Users of College electronic communications facilities **must** identify explicitly in these communications whether they are speaking for the College or as individuals.

3.5.1 Unlawful Activities

These are activities defined as illegal or unlawful under public law.

3.5.2 Business Enterprises

Electronic communications facilities are not to be used for commercial purposes not under College authority.

3.5.3 Endorsements and Promotions

Facilities are not to be used for unauthorized endorsements of outside entities, goods, and services.

3.5.4 Personal Financial Gain

No person may use College electronic communications systems for personal financial gain (except as permitted under applicable human relations policies).

3.5.5 Capacity Overload

Electronic communications systems should not be used for purposes that can reasonably be expected to cause, directly or indirectly, excessive loading of College or others electronic facilities.

3.5.6 College Policies

No one may use electronic communications systems that violate other College policies, procedures, and guidelines. These include, but are not limited to, policies, procedures, and guidelines regarding intellectual property, sexual and other forms of harassment, hate crimes, privacy, financial integrity, and substance abuse.

3.5.7 Other

No one may use electronic communications systems for other functions that fall under personal use inconsistent with Allowable Use (defined above). These may include, but are not limited to, soliciting or proselytizing for political causes, religions, and charities not sanctioned by College leadership.

3.6 Disclaimers

Users of College electronic communications facilities are expected to identify explicitly (if it is not obvious implicitly) in these communications whether they are speaking for the College or as individuals. Although one may identify her/his affiliation with the College in such communications, it may be necessary, should it not be clear from the context of the communications, for the user to make a specific disclaimer indicating that the person is speaking for her/himself and not the College. The following should set the standard for the minimum content for such disclaimers:

3.6.1 Sample Disclaimer

“The content and the opinions expressed in these communications are the opinion of the writer, not College of DuPage, Community College District #502, its Board of Trustees, or members of its staff.”

3.7 False Identities

Users of College electronic communications services are obligated to identify themselves and not use the identifiers of other individuals. A pseudonym may be used provided that its intent is not to falsify identity. Anonymous electronic communications are protected in the case of whistle-blowing and for use in moderated electronic discussions provided the manager or coordinator of discussions is identified by name and assumes responsibility for such anonymous postings.

3.8 Personal Use

The College strongly discourages personal use of all College electronic communications facilities including, but not limited to, e-mail, voice telephones, FAX, two-way radios, web boards, electronic bulletin boards, and list-servs. The College assumes no responsibility for any loss or damage sustained by an individual who uses electronic communications facilities for personal reasons. College systems may not provide the time-sensitivity or confidentiality that personal users may expect from their own systems. Those who make use of College electronic communications must not:

3.8.1 Interfere with College Electronic Communications Facilities

Such use must not directly or indirectly interfere with the College's operations of electronic communications facilities.

3.8.2 Incur Costs

Such use must not subject the College to measurable, avoidable costs (for which the person may have to reimburse the College).

3.8.3 Compromise the College Mission

Such use must not interfere with instruction, instructional support, and other aspects of the College mission.

3.8.4 Clash with Job Duties

Such use must not interfere with the user's job duties or those of others.

3.9 Unsolicited Communication

The College will meet the standards set by public law for unsolicited communication.

3.10 Accessibility

All electronic communications intended to support the College mission of instruction and community service shall be accessible to allowable users with disabilities. In compliance with law and College policies, this use must be financially and administratively practical. If technological solutions are not practical, alternative methods of communication shall be made available to such users.

3.11 Intellectual Property

All College electronic communications shall conform to the law and College policies regarding the protection of intellectual property including, but not limited to, copyright, patents, and trademarks.

Users who go beyond federal definitions of "fair use" must seek and secure appropriate permission to distribute protected material, no matter what the form, including, but not limited to, text, photographic images, audio, video, graphic illustrations, and computer software.

All users must assume that all written, printed, or electronically reproduced materials are copyrighted or protected unless there is an explicit statement to the contrary or the material is clearly in the public domain.

3.12 E-Mail

The College uses e-mail not only for dissemination of “official” information, but also for the everyday transmittal of information to insure the smooth working of the College. E-mail’s primary use is to support the business and mission of the College. The enormous growth in e-mail volume necessitates that all staff make common sense decisions about using appropriate media choice for communications. Additionally, e-mail provides a ready record of all voice mail messages through an integrated messaging system. Users who use voice mail should be fully aware that such messages may be archived by the person to whom they are sent. Those who retain such messages should hold them in accordance with all other standards of use and policies governing electronic communications. The College e-mail system provides the capability of “attaching” documents and files of many media to e-mail correspondence. Such attachments are also subject to the same standards and policies as all other electronic communications.

To help facilitate the dissemination of information to all college employees, an e-mail distribution list titled “Official Communications” has been created. Electronic communication that supports College business and impacts all college staff will be sent through this e-mail distribution list. This e-mail distribution list may only be used by the College President, Vice-Presidents, and other authorized college staff. Any college staff seeking to become authorized to use this e-mail distribution list must be given permission by their Vice-President.

3.12.1 Unauthorized E-Mail Practices

In addition to the general policies and guidelines governing electronic communications, e-mail users should not engage in the following activities.

3.12.1.1 Chain Letters

Users should not use College communications systems to initiate, send, or forward electronic mail chain letters.

3.12.1.2 “SPAM”

Users of College electronic systems should not create or send “spam;” i. e., users list-serves or similar broadcast systems for purposes beyond their legitimate scope to distribute unsolicited electronic mail.

3.12.1.3 “Letter Bombs”

Users of College electronic systems should not create or send “letter bombs;” i. e., send messages for the purposes of disrupting a recipient’s electronic communications. These “letter bombs” include, but are not limited to, extremely large messages or repetitive sending of similar messages.

3.12.1.4 Disruption

Users of College electronic systems should not intentionally or negligently use electronic telecommunications facilities to disrupt the College or others electronic systems. Such disruptions would include the intentional sending/forwarding of a computer virus.

3.13 Electronic Bulletin Board

The College maintains sophisticated electronic bulletin board systems that carry both informational and “official” content. These include web-portal and web-based systems. They are to be used for College-wide business information distribution. The content is broad ranging from Board of Trustees meeting minutes to casual news of interest to the entire College community. Some of these electronic bulletin board systems allow staff to subscribe to categories of information based on their interest. All electronic bulletin board systems are subject to the same standards of use and policies that govern all other electronic communications.

3.14 Public and Shared Folders

The College provides public and shared messaging within the e-mail system. The system allows users to create and disseminate information through the use of “public” and “shared” folders that can be both “official” and informational. Use of these electronic folders is subject to the same standards of use and policies that govern all other electronic communications.

3.15 Network Storage for Department and Individual Use

The College provides its departments and staff members shared and personal disk space on its servers to facilitate College operations and provide a high level of security for data stored in such space. There is a formal process for requesting such space, and use of it is governed by the same standards and policies that govern all other electronic communications.

3.16 Distribution

A variety of College electronic communications systems (most conspicuous is e-mail) provide means of distribution of communications to a pre-selected list. Such lists must be developed and protected in accordance with standards and policies established for all other electronic communications, and lists restricted to specific groups or constituencies in the College will be protected by appropriate procedures.

3.17 Approval and Authorization

Users must seek and receive proper approvals from designated College units for permission to establish such communications and must conform to established policies and guidelines. Forms to apply for such approvals will be available from the appropriate units and/or on the appropriate electronic bulletin board system.

3.18 Responsible Person

All users of College electronic communications should be aware that there is a person (manager, moderator, coordinator, or other) who assumes the responsibility for access to, and content of, such services that involve sharing (e. g., e-mail, list servs, newsgroups, network disk space, public/shared folders, and electronic bulletin boards) to assure that use of such services meets established College policies and guidelines.

3.19 Web Pages

Web Pages have assumed an important communication, marketing, and instructional role for the College and their use has grown vigorously. Continued dramatic growth is anticipated. Realistically, the College cannot always design, approve, and monitor every page on the College electronic facilities. Unit managers or individual users shall assume responsibility for these pages that must conform to the following guidelines:

3.19.1 Identification

No anonymous web pages are permitted. Every web page must carry the name of a unit, sub-unit, program, committee, or individual responsible for the page.

3.19.2 Official Web Pages

Web pages that contain official announcements and information for the College shall carry a distinct identifier including, but not limited to, text, logo, trademark, legal notice, signature, and/or seal to give them a different “look and feel” from pages that carry other informational traffic. No other College web pages may use these distinct identifiers.

3.19.3 Individual Web Pages

Many College faculty members maintain “individual” web pages for use by their students, former students, potential students, professional colleagues, and the public. Their purpose is to foster the College business of learning and learning support. These pages are subject to all appropriate College policies and guidelines. No personal (those that have no institutional use) web pages are permitted on College electronic communications facilities.

College faculty and staff must identify themselves by name and assume full responsibility for the content and maintenance of these individual web pages.

3.20 Course Management System(s)

This software application(s) provides automation and electronic convenience to the business of managing both classroom and non-traditional course delivery. To work effectively, course management systems rely on solid electronic communications facilities. All policies and guidelines including, but not limited to, the College’s Electronic Communications Policy and Guidelines apply to the use of these course management systems. Because it is an “official” function of the College, following the policies and guidelines for use of such systems is a critical responsibility for faculty, staff, and students. Students should be aware that use of electronic

course management systems does not change their basic rights and responsibilities as defined in the College catalog.

3.21 Voice Systems

The College maintains a voice system, a related voice-mail system, and an integrated message system using the College e-mail system to access and store voice mail messages and faxes. College staff and students who use College telephones for voice and FAX communication are strongly urged to familiarize themselves with College policies and guidelines regarding electronic communications and the body of very specific law governing their proper use. There are clear guidelines in the law concerning, but not limited to, privacy, recording of telephonic communications, use of improper language, harassment, and wire fraud.

Personal use of telephones is defined above (3.8), and the measurable costs of telephone communications (e. g., long distance charges) may be recovered by the College. The College has the right to add a service fee should recovery of such cost data involve additional expense. The College strongly urges that those who use College voice systems for personal use charge, whenever possible and practical, these calls involving exceptional charges (e. g, long distance) to personal phones or personal credit cards.

3.22 Broadcast Radio and Television

3.22.1 Licensing

Operation of any broadcast radio and television operation requires Federal Communications Commission licensing. Application for, maintenance of, and adherence to, licensing requirements are the responsibility of the managers of radio or television operations. Such license applications must be approved by the Vice President of Information Technology and the President of the College.

3.22.2 Broadcast Interference

Users of radio frequencies (including College-owned two-way radios, wireless networks, cell phones, and other devices) shall operate their equipment in a manner that does not interfere with other operators.

3.22.3 Broadcast Content

Because such broadcast content is deemed an “official” presence of the College, it is subject to all appropriate College policies, guidelines, and oversight.

3.23 Cable Television

College use of cable television access should conform to all appropriate College policies and guidelines, standards set by the cable carriers, and applicable public laws. College use of cable outlets is considered an “official” use.

3.24 Streaming Audio and Video

Computers now have the ability to “re-broadcast” College radio and television signals. These signals are an “official” presence of the College and must meet not only standards set by public

law and the web carriers, but also all appropriate College policies and guidelines. Those who originate messages using this capability must be aware of, and comply with, the rules governing intellectual property with particular note made of policies governing “copying” of copyright materials.

3.25 Other Wireless Devices

All wireless electronic devices that form part of the College’s electronic communications systems not listed specifically above are subject to the same general policies, procedures, and guidelines as the use of “wired” electronic communications technologies.

3.26 Penalties

Use of, and access to, College electronic communications is a privilege. This privilege can be restricted wholly or partially without prior consent of the electronic communications user when the College deems that these facilities have been used in an inappropriate manner that may be defined by, but not limited to, College policies and public law.

4.0 Privacy

4.1 Introduction

Free and open communications are the hallmark of good education, and the College maintains a strong commitment to academic freedom, shared governance, freedom of speech, and the privacy of information with which it is entrusted. These commitments can be more complex to maintain in the world of electronic communications.

The College does encourage electronic communications and does not routinely inspect, monitor, or disclose the content of electronic communications without the holder's consent. However, because the College may deny access to electronic communication services for, but not limited to, improper use, capacity, and technology, it may inspect, monitor, or disclose electronic communications under appropriate circumstances.

College policies on maintaining the privacy of its printed and electronic records also apply to all types of electronic communications. However, the College cannot take responsibility for all the challenges modern electronic technologies pose to privacy. Similarly, it cannot assume responsibility for the negligence or inattention to issues of privacy that are the responsibility of users of the electronics communications systems (refer to Guideline 4.3 below).

4.2 Exceptions to Privacy Standards

4.2.1 Protected Information

Two specific categories of information are protected by law. When electronically protected information is gathered, the person whose information is gathered, and subsequent users of that information, should be informed of the protected nature of that information.

4.2.1.1 Individual Identity

This is information that personally identifies an individual.

4.2.1.2 Student information

This information is defined in federal law by the Family Educational Rights and Privacy Act of 1994.

4.2.2 Other Limits on Privacy

The privacy of electronic communication is not absolute. It is limited by:

4.2.2.1 Freedom of Information Laws

This body of law is designed to protect the public's right to know about the public business through access to public records.

4.2.2.2 Release of College Records

All College employees are required to comply with College requests for copies of written, printed, or electronic records in their possession that pertain to the business of the College or the disclosure of which is required to comply with applicable laws, regardless of whether such records reside on a computer

housed or owned by the College. Failure to comply with such requests can lead to the conditions requiring Access Without Consent detailed in Guideline 4.4 below.

4.2.2.3 Inspection of Electronic Communications

Users of College electronic communications should be aware that electronic systems support personnel monitor transmissions and/or observe transactional information from time to time to ensure proper functioning of College electronic communications facilities and services. Unless there are reasons to do so defined by public law and/or College policies, procedures, or guidelines, College personnel are not permitted to hear, see, or read the contents intentionally. However, it is possible that College personnel might see the contents of an electronic communication inadvertently. These support personnel may not search or peruse in detail such transactional information not germane to their foregoing purpose or to disclose or otherwise use what they have heard, seen, or read.

It should be noted that systems personnel might be required to inspect the contents of electronic communications and transactional records when redirecting or disposing of undeliverable electronic communications or other like activity. The working standard is to use the least invasive level of inspection. These employees are not permitted to disclose personal or confidential information, except in cases where such disclosure amounts to good faith attempts to route the otherwise undeliverable electronic communication to its intended recipients. Re-routed electronic communications normally should be accompanied by notification to the recipient that the electronic communication has been inspected for the purpose of finding the addressee.

4.2.2.4 Back-up Artifacts

Users of electronic communications facilities should be aware that erasure or deletion of electronic communications stored on devices under their control does not necessarily destroy all copies, some of which might be backed-up on other devices. Such copies that can be retrieved are subject to disclosure governed by College policies.

4.3 User Responsibilities

The College is committed to doing its best to maintain the security of its electronic communications within the bounds of the law, technical feasibility, and cost. Users of these facilities bear a significant part of the responsibility for this security. Users should make careful judgments about the security of a given mode of electronic communication. Essentially, the more mature the means of communication; e. g. the United States Postal Service or voice telephones, the more privacy one might expect, both through technology and the body of law that has grown up around these older technologies. Newer forms of communication may be technologically less secure and may lack the buttressing laws to protect the user. Users should view communications as a hierarchy with declining potential for privacy through a combination of both technological and legal considerations:

- First class letters and telephone conversations afford a high degree of privacy and are both well protected by law.

- E-mail can be technologically secure, but the body of law protecting it is far from complete. Also, its technology allows the recipient to easily turn a private message into one with broad circulation, revise it in the forwarding process, or otherwise tamper with intent or context.
- Unprotected web pages, broadcast and narrowcast radio and television, and systems like list-servs, bulletin boards or newsgroups are by nature intended to be relatively open forms of communication. Users should have low, or no, expectations of privacy.

It is up to the communicator to choose a means of communication that gives the user the highest comfort level of privacy. Ultimately in any environment, communications by its very nature in any form cannot be fully protected. Users should be aware that passwords do not always protect communications. Password users often do share them or leave them accessible to others. Recipients may photocopy letters, illegally record phone calls, re-send e-mails or break assurances of discretion in many different ways. Skilled “hackers” bent on malice can make a mockery of a user’s right to privacy. The user will have to make a choice of media. To use good judgment in that choice is the responsibility of the communicator.

Additionally, users should be aware that certain work habits invite breaches of privacy. Posting one’s e-mail address on list-servers or bulletin boards is one example. Leaving one’s files on computers in public labs is another. Users should also be aware that what may seem secure may not be. Search engines can find web pages linked to no other pages. Random surfing of the web is likely to leave an auditable trail of visits to web pages that a web host may use to secure information about the “surfer.”

Although the privacy of telephone conversations is protected by law, and it is illegal to record or monitor audio or visual telephone conversations without advising the participants the call is being monitored or recorded, under public law courts can approve such monitoring or recording.

The public law may allow the College to monitor and record telecommunications by employees to evaluate customer service, measure workload, or other business purposes. However, employees and those whose communication is being monitored and/or recorded must be informed that such monitoring or recording may take place. Students and others who communicate with the College must have access to an alternative method of doing business with the College should they not wish to submit to such monitoring.

All telephonic communications can leave transaction records. College employees should be aware that supervisors can access these records of calls made from College telephones and that such records may be used for administrative purposes.

Users should be aware that unannounced listeners on speakerphone calls or on conference calls might compromise telephonic communications privacy. Voice mail systems sometimes have back-up features that retain messages or information even though the voice mail user may have erased the messages. The College integrated messaging system does allow the receiver of voice mail or faxes to archive such communications.

Conversations on cellular and cordless phones cannot be assumed to be private. Monitoring of such conversations, particularly on analog lines, is comparatively simple for those with malicious intent. Also, cellular phones are often used in public places, and conversations often reach the sharp ears of eavesdroppers.

4.4 Access Without Consent

The College shall secure the consent of the user prior to any inspection, monitoring, or disclosure of College electronic communications in the holder's possession, with the following exceptions:

4.4.1 Exceptions

4.4.1.1 Public Law

Consent is not necessary when required by, and consistent with, public law.

4.4.1.2 Evidence of Crime

Consent is not necessary when there is substantiated reason to believe violations of the law have taken place.

4.4.1.3 Compelling Reasons

Prior consent may not be necessary when there are compelling circumstances as defined in 7.0, Appendix: Definitions.

4.4.1.4 Critical Operational Circumstances

Prior consent may not be necessary under time-dependent, critical operational circumstances as defined in 7.0 Appendix: Definitions.

4.4.1.5 Violations of College Policy

Prior consent is not necessary where there is substantiated reason to believe that violations of College Policies have taken place.

4.4.2 Authorization

Except in emergency situations defined in 7.0, Appendix: Definitions, and pursuant to Guidelines 4.2 above, authorization to inspect, monitor, or disclose electronic communications in a holder's possession for other than normal administrative or maintenance reasons must meet the following requirements:

4.4.2.1 Timing

Authorization must be issued in advance.

4.4.2.2 Form

Authorization must be in writing.

4.4.2.3 Legal Counsel

Authorization must be sought with input from the College attorney.

4.4.2.4 Signatory

Authorization must be signed by the Vice President of Information Technology or the President of the College.

4.4.3 Guidelines

These guidelines provide that once an employee is delegated the task of accessing electronic communication without consent, that task may not be re-delegated unless the above sequence is repeated. In all cases, the authorization carries with it the explicit direction that the least (minimal) perusal of contents with the least action necessary to resolve the situation be used. In both letter and spirit such inspection, monitoring, and disclosure are not to be “fishing expeditions.”

4.4.4 Emergencies

In emergency situations, the responsible authority shall, at the earliest opportunity that is lawful and consistent with other College policy, notify the affected individual of the actions taken and the reasons for the actions taken.

4.4.5 Notification

In non-emergency cases, the responsible authority shall, at the earliest possible opportunity that is lawful and consistent with other College policy, notify the affected individual of the actions taken and the reasons for the actions taken.

4.4.6 Compliance with Law

All actions taken shall be fully compliant with the law and all College policies. Advice of College Legal Counsel must always be sought prior to any action involving electronic communications that meet the following criteria:

4.4.6.1 Location

This is information stored on equipment not owned or housed on College property.

4.4.6.2 Privacy Laws

This information is protected under the federal Family Educational Rights and Privacy Act of 1974 and other appropriate laws governing privacy of customer information.

5.0 Security, Records, and Archiving

5.1 Introduction

The security of electronic records is a paramount concern of the College. In the networked, interconnected world created by modern technologies (including the web), privacy and security of data and communications are very much under threat. These threats can be willful, as in the work of hackers, or accidental through careless users. They can be the result of the failure of complex systems or the lack of currency in security hardware, software, and guidelines.

5.2 User Responsibility

As in the case of privacy, the security of electronic communications begins and ends with the activities of responsible users. Sophisticated security systems cannot guard against the problems created by machines that are left running in a public place, by sloppy care of passwords, and by inattention to the cautions that working in a networked world dictate.

5.3 Access

Any access/use of College of DuPage electronic communications systems is restricted to duly authorized individuals only. The College can restrict usage at its relatively "open" facilities in public locations on the campus. Any unauthorized access/use by any individuals, including administrators, faculty, classified staff, students, and the public, of the computer systems, computer network, computer programs, computer software, computer supplies, documentation, data, and/or College electronic communication systems will be subject to disciplinary action, civil action, and or criminal prosecution.

5.4 Security Breaches

Any purposeful breaches of College computer or electronic communications security systems by staff, students, and/or members of the public can result in discipline that could include termination, expulsion, revocation of access to electronic communications, and other appropriate disciplinary actions. Some breaches can result in criminal or civil remedies. Consistent accidental or negligent breaches in security can result in disciplinary guidelines by management that, in circumstances defined by security guidelines, result in suspension or termination.

5.5 Records and Archiving

A significant percentage of the College records exist only in electronic form. Given the volume of such data and information, it is unrealistic to think that these records can be translated to paper and stored. Therefore, users of electronic communications should know what records they are required to retain, to dispose of, to archive, or to pass on. Electronic records, such as paper files, can have an official status, and their willful destruction or misuse may be subject to the same discipline that governs a College staff person's use of paper records. These actions may also result in civil or criminal penalties.

6.0 Uses

6.1 Employee Training

These Guidelines will be part of new employee orientation and will become part of the on-going training for current College staff. Electronic communications technology and its proper use are necessary for staff to work effectively. These technologies are to be used to do the business and fulfill the mission of the College.

7.0 Appendix: Definitions

Access/Use

Access/Use means: to approach, to instruct, communication with, store data in, retrieve or intercept data from, or otherwise make use of, any resources of computer, computer system, computer network, or electronic communications device or system that is part of the College computing assets, whether or not owned by the College or on College property. Information that is the property of the College is also covered by this access/use definition even though that information may be on computing assets not owned by the College. Only authorized personnel can display, change, copy, duplicate, print, delete, destroy, and/or access data, documentation, and/or computer programs stored in any computerized form or make any authorized use of the computer system.

College Electronic Communications Record

A College record in the form of an electronic communication, whether or not any of the electronic communications facilities utilized to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print the electronic communications record are owned by the College. This implies that the location of the record, or the location of its creation or use, does not change its nature: (1) as a College electronic communications record for purposes of this or other College guidelines; and (2) as having potential for disclosure under public law.

Until determined otherwise, or unless it is clear from the context, any electronic communications record residing on College-owned or College-controlled telecommunications, video, audio, and computing facilities will be deemed to be a College electronic communications record for purposes of this Guideline. This would include personal electronic communications. Consistent with the principles of least perusal and least action necessary and of legal compliance, the College must make a good faith effort to distinguish College electronic communications records from personal and other electronic communications in situations relevant to disclosures under public law and other laws, or for other applicable provisions of this Guideline.

College Electronic Communications Systems or Services

Electronic communications systems or services owned or operated by the College or any of its sub-units or provided through contracts with the College.

College Record

A "public record" is defined in College policy and public law. Public records include writing or other forms of recording that contain information relating to the conduct of the public's business in materials prepared, owned, used, or retained by the College regardless of physical form or characteristics. Except for certain defined situations, such College records are subject to disclosure under the College policies and public laws.

Records held by students, including electronic communications records, are not necessarily College records unless such records exist pursuant to an employment or agent relationship the student has, or has had, with the College.

Compelling Circumstances

Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of

College policies, and/significant liability to the College or to members of the College community.

Electronic Communications

Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services.

Electronic Communications Facilities

Any combination of telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

Electronic Communications Records

Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. This definition of electronic communications records applies equally to the contents of such records, attachments to such records, and transactional information associated with such records such as headers, summaries, addresses, and addressees.

Electronic Communications Systems or Services

Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

Emergency Circumstances

Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.

Holder of an Electronic Communications Record or Electronic Communications Holder

An electronic communications user is one who, at a given point in time, is in possession (refer to definition below) or receipt of a particular electronic communications record, whether that electronic communications user is the original creator or a recipient of the content of the record.

Official Communications

Electronic communications, or any other form of communications, that supports College business and impacts the entire college staff.

Possession of Electronic Communications Record

An individual is in possession of an electronic communications record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an electronic communications record that resides on an electronic communications server awaiting download to an addressee is deemed, for purposes of this Guideline, to be in the possession

of that addressee. Systems administrators and other operators of College electronic communications services are excluded from this definition of possession with regard to electronic communications not specifically created by, or addressed to, them. Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

Substantiated Reason

Reliable evidence indicating that violation of law or of College policies probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

Time-Dependent, Critical Operational Circumstances

Circumstances in which failure to act could seriously hamper the ability of the College to function administratively or to meet its instructional obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance.

User of Electronic Communications Services

An *Electronic Communications User* is an individual who makes use of electronic communications services; whether the purpose be to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic communications with the aid of electronic communications services.

Receipt of electronic communications prior to actual viewing is excluded from the definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the electronic communications record.

Web-Portal System

A web-portal system presents information from diverse sources in a unified way. Apart from the standard search engine feature, web portals offer other services such as e-mail, news, stock prices, information, and entertainment. Portals provide a way for enterprises to provide a consistent look and feel with access control and procedures for multiple applications, which otherwise would have been different entities altogether. Examples of a web portal are MSN, Yahoo!, AOL, or Google.

Web-Based System

A web-based system is an application that is accessed via a web browser over a network such as the Internet or Intranet.