

POLICY MANUAL

| | | | |
|------------------------------------|------------------------------------|-----------------------|----------------------------------|
| Policy: Email (proposed) | | Policy No. TBD | Page: 1 of 14 |
| | | Issue No. 1.0 | Issue Date: Oct. 12, 2001 |
| Scope: Global | Effective Date: Jan 1, 2002 | Approved By: | |
| | Expiration Date: N/A | Title: Provost | |

Sinclair Email Policy (Proposed)

Effective: Immediately as Interim Guidelines; Adoption as Policy by Board of Trustees estimated January 1, 2002

Policy Statement Summary

- IV. A. Electronic mail services are provided by the College for academic and administrative purposes.
- IV. B. All electronic mail systems and services, including email messages, are college property.
- IV. D. Users are responsible for the security of their password and accountable for use of their ID.
- IV. F. Each user will have a default server-based mailbox limit. Exceptions to this limit will be coordinated through the Help Desk.
- IV. G.1. Email use for unlawful activities is prohibited.
- IV. G.2. Offensive, demeaning, harassing, or disruptive messages are prohibited.
- IV. G.3. Email use for personal monetary gain is prohibited.
- IV. G.4. Email use for solicitation or literature distribution for non-Sinclair purposes is prohibited.
- IV. G.5. Users sending messages containing personal or student record information must comply with the Family Educational Rights and Privacy Act.
- IV. G.6. A user will not attempt to gain unauthorized access to another user's email account.
- IV. H. The use of server-based distribution lists such as "All Sinclair Mail Users" is restricted.
- IV. J. Email services will not be used to cause excessive strain on resources or cause interference; chain letters, spam, and letter/mail bombs are prohibited.
- IV. K. Email may be used for incidental personal purposes providing it does not interfere with official college use.
- IV. L. Email communications are not considered private despite any such designation either by the sender or the recipient.
- IV. M. Users should be wary of and take precautions to avoid introducing viruses and malicious code to the college network.
- IV. N. The College has the right to monitor its email system—including an employee's mailbox—at its discretion in the ordinary course of business.
- IV. O. Users should consult records management staff in regards to how records management policies apply to material contained in electronic mail.
- V. Any user who violates the policy shall be subject to disciplinary actions.

Sinclair Email Policy

Table of Contents

I. INTRODUCTION 3

II. PURPOSE 3

III. SCOPE 3

IV. POLICY STATEMENT 3

 A. Purpose 4

 B. College Property 4

 C. Users 4

 D. Account Responsibility 4

 E. Email Addresses 4

 F. Mailbox Space Limits 4

 G. Specific Restrictions 5

 H. Email Distribution Lists 5

 I. Representation 5

 J. Interference 6

 K. Personal Use 6

 L. Confidentiality 6

 M. Security 7

 N. Access and Disclosure 7

 O. Archiving and Records Retention 8

V. POLICY VIOLATIONS AND SANCTIONS 8

VI. POLICY RESPONSIBILITY 8

VII. PROCEDURES 9

GLOSSARY 10

INDEX 13

I. Introduction

This policy specifically addresses issues related to the use of electronic mail services. Sinclair Community College recognizes that principles of academic freedom, freedom of speech, and privacy hold important implications for electronic mail and electronic mail services. Use of this medium is encouraged for academic and administrative purposes. Sinclair Community College provides all electronic mail services in support of the learning, research, and community/public service mission of the College and all administrative functions that support this mission.

II. Purpose

The purpose of this policy is to assure:

- The Sinclair Community College community is informed about the applicability of policies and laws as related to electronic mail services.
- Electronic mail services are used in compliance with those policies and laws.
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail.
- Disruptions to College electronic mail and other services and activities are minimized.

III. Scope

This policy applies to:

- All electronic mail systems and services provided or owned by the College.
- All users, holders, and usage of the College email services.
- All College email records in the possession of all users of electronic mail services provided by the College.

IV. Policy Statement

This section contains specific provisions for the Sinclair Email Policy.

- A. Purpose
- B. College Property
- C. Users
- D. Account Responsibility
- E. Email Addresses
- F. Mailbox Space Limits
- G. Specific Restrictions
- H. Email Distribution Lists
- I. Representation
- J. Interference
- K. Personal Use
- L. Confidentiality
- M. Security
- N. Access and Disclosure
- O. Archiving and Records Retention

A. Purpose

Electronic mail services are provided by the College for academic and administrative purposes. The College encourages the use of its electronic mail services to share information, to improve communication, and to exchange ideas in support of these purposes.

B. College Property

All electronic mail systems and services, including email messages, are the property of Sinclair Community College.

C. Users

1. Users are all College faculty and staff.
2. Network Access, including access to electronic mail services, is issued automatically to all Sinclair faculty and staff after they have been entered into the Human Resources system.

D. Account Responsibility

Users are responsible for the security of their password and accountable for any activity resulting from the use of their user ID. If a user suspects or discovers that someone else knows their password, the user should change the password immediately.

E. Email Addresses

1. Users may have only one personal electronic mailbox and email address.
2. The standard format for email addresses is: `firstname.lastname@sinclair.edu`.
3. In cases of duplicate names, middle names or hyphenated last names will be used in the email address.
4. Special email addresses (departmental email addresses, etc.) must be requested through the Help Desk.

F. Mailbox Space Limits

1. Each user will normally have a default server-based mailbox limit for Microsoft Exchange (Outlook) items such as email messages, calendar items, and journal items. Requests for additional server space beyond the default limit must be coordinated through the Help Desk and require written approval from the appropriate Dean or Director.
2. A warning will be issued when a user's mailbox is within ten percent of its capacity. A second warning will be given if the mailbox grows to within two percent of its capacity. After the second warning the user will not be able to send any mail. The user must then delete messages or move them to personal folders on the hard drive to be able to send email. If the mailbox reaches the imposed limit, the user's email account will cease to function; the user will not be able to send or receive email. The user must then delete mail items or move them to personal folders stored on the hard drive to restore email functions.

G. Specific Restrictions

1. Use of college electronic mail services for unlawful activities is prohibited.
2. Offensive, demeaning, harassing, or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the College's Equal Employment Opportunity policy or Harassment policy.
3. Use of the College's electronic mail services for personal monetary gain is prohibited.
4. Email will not be used to solicit students or employees for any purpose, or to distribute literature for any person or organization, except United Way, Culture Works, and Sinclair Community College. The use of such messages is guided by the Campus Access Policy.
5. Users sending messages containing personal information or student record information must comply with Family Educational Rights and Privacy Act (FERPA) guidelines. All student information must be treated as confidential, even public or "directory information" may be subject to restriction. Release of information contained in a student's record without written consent is a violation of Sec. 438 Public Law 90-247. Any requests for disclosure of student information, especially from outside the College, should be referred to the Office of Registration and Student Records. Individual copies of the Student Records Policies and Procedures for Sinclair Community College are available from the Office of Registration and Student Records.
6. A user will not attempt to gain unauthorized access to another user's email account.

H. Email Distribution Lists

1. The use of the "All Sinclair Mail Users" option is limited to email messages for academic and administrative uses. This option gives users the ability to send email to all Sinclair mail users. Good judgment should be exercised in the use of this option. The message should be campus-wide in nature. It should also contain material that is time-sensitive and would not otherwise be published in another form such as the President's Bulletin. Examples of inappropriate use include garage sale announcements, non-Sinclair sporting event tickets for sale, solicitations for a favorite charity, etc. If users are unsure if a message should be distributed to all users, they should obtain approval from their supervisors. Supervisors should obtain approval from the appropriate manager, dean, or director. Final approval for an "All Sinclair Mail Users" message rests with the respective Vice President.
2. Email distribution lists will be created on a network server for sanctioned committees or teams (list owner) approved by the appropriate Dean or Director. The lists will be used for academic and administrative purposes. Email distribution lists will be maintained by their assigned owners. The list owner will establish the scope and distribution of each list prior to its creation. The list owner will be responsible for assuring that users follow the list guidelines.

I. Representation

1. Electronic mail users will not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the College unless explicitly or implicitly authorized to do so.

2. Where appropriate, a disclaimer will be included unless it is clear from the context that the author is not representing the College. An example disclaimer is:

“The opinions or statements expressed here are my own and should not be taken as a position, opinion, or endorsement of Sinclair Community College”

3. Users will not use a false identity in electronic mail services. “Spoofing”, i.e. constructing an electronic mail communication so it appears to be from someone else, is prohibited.

J. Interference

Electronic mail services will not be used in any way or purpose that could cause, either directly or indirectly, excessive strain on computing facilities or cause interference with others’ use of the electronic mail systems. These include but are not limited to:

- Chain Letters: e.g. “Send this message to ten more people”.
- “Spam”: unsolicited, usually commercial, email sent to a large number of email addresses.
- “Letter Bombs”: resending the same email repeatedly to one or more users to interfere with the recipient(s) use of email.
- Sending excessively large email attachments that could be transmitted by other means such as network shared areas, public folders, or floppy and zip disks.

K. Personal Use

1. Electronic mail services can be used for incidental personal purposes provided that it does not interfere directly or indirectly with the operation of College computing facilities or electronic mail services; it does not burden the College with noticeable cost; and it does not interfere with the user’s employment obligations to the College.
2. Users should assess the implications of their decision to use College electronic mail services for personal use. Email records resulting from such personal use may be subject to the archive and record retention requirements of the College. Email records resulting from personal use are also backed up during routine system backups.

L. Confidentiality

1. Email communications are not considered private despite any such designation either by the sender or the recipient.
2. Confidentiality of electronic mail services cannot be assured. Confidentiality may be compromised by applicability of law or policies, including this policy; by unintended redistribution; or because of the inadequacy of current technologies to protect against unauthorized access. Operators of College electronic mail services are expected to follow sound professional practices in providing security of electronic mail data. However, since the protections are not foolproof, the security and confidentiality of email cannot be guaranteed. Users should exercise extreme caution in using email to communicate confidential or sensitive information.

3. The existence of passwords and “message delete” functions does not restrict or eliminate the College’s ability or right to access electronic communications. The delete function does not eliminate the message from the system. Systems are “backed up” on a routine basis to protect system reliability and integrity and to prevent potential loss of data. The backup process results in the copying of data onto storage media that is retained for periods of time and in locations unknown to the sender or recipient of the email.

M. Security

1. Users will not share their password, provide access to an unauthorized user, or access another user’s mailbox without authorization (such as when granted delegate rights).
2. Messages sent to recipients outside of Sinclair, if sent over the Internet, are not encrypted (software used to encode and protect electronic data), and are not secure. The use of encryption software by users requires prior IT approval.
3. Users should be aware that current technology used on the Internet does not provide guarantees that a user is who they say they are and that no one other than the authorized person can receive the information that is requested. It is not possible to ensure that the person on the other end of a communication is who they say they are because of the ability to fake or "spoof" an IP address or the ability to listen to or “sniff” other people’s communication.
4. Users should be wary of and take precautions to avoid introducing viruses and malicious code to the college network. Attachment files received via email should be scanned using current anti-virus software before opening. Suspicious messages such as those received from unknown sources or those received from known individuals but with unlikely or inappropriate subject lines (for example “I Love You” from your supervisor or instructor) should be reported to the Help Desk and should not be opened.

N. Access and Disclosure

1. The College reserves the right to monitor its email system—including an employee’s mailbox—at its discretion in the ordinary course of business.
2. The College reserves the right to inspect and disclose the contents of electronic mail:
 - a. In the course of an investigation triggered by indications of misconduct or misuse,
 - b. As needed to protect health and safety,
 - c. As needed to prevent interference with the academic and administrative missions of the College, or
 - d. As needed to locate information required for College business that is not more readily available by some other means.
3. Court order or law enforcement investigation may also require the examination and release of electronic mail data.
4. Supervisor Access to Employee Network Files, including email.
 - a. For security purposes, IT will normally only reset passwords for the account’s owner. However, in the absence of an employee, the supervisor can obtain access to the employee’s network files if conditions warrant. Access to network files includes the employee’s home directories, email messages, shared areas, etc.
 - b. It is important for supervisors to arrange with the employee for any necessary access

- to network files when they leave the College, are on vacation/sick leave, or absent for any other reason. This may involve the employee providing the supervisor with a password-protected shared area on their system, transferring necessary files to the supervisor's network area or a common network area, or any other appropriate method.
- c. Where these arrangements have not been made, and the supervisor requests access to the employee's network files through the IT Help Desk, formal approval from the appropriate Dean or Director must be included with the request.
 - d. With this authorization, IT will either provide access to a specific requested file or change the employee's network password and provide a new password to the supervisor. The supervisor is then responsible for explaining the situation and reviewing this information with the employee upon their return to their office.

O. Archiving and Records Retention

1. College records management policies do not distinguish among media with regard to the definition of College records and electronic mail records that are subject to these policies. Users should consult records management staff in regards to how records management policies apply to material contained in electronic mail.
2. The College does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Backup files are stored for a limited time period. Electronic mail is only backed up to assure system integrity and reliability, not to provide for future long-term retrieval.
3. Email users should be aware that it is generally not possible to ensure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part due to the changing nature of electronic mail systems.
4. Email users and those in possession of College records in the form of electronic mail are cautioned to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Electronic mail should be transferred to a more lasting medium/format where long-term accessibility is an issue. When in doubt about how to maintain long-term electronic mail records, users should contact College records management staff for guidance.

V. Policy Violations and Sanctions

Any misuse of email, including but not limited to the sending of harassing, threatening, inappropriate, or offensive material via this medium, will result in discipline up to and including termination of employment under applicable College policy.

VI. Policy Responsibility

The Board of Trustees of Sinclair Community College approves policy recommended by the President and has the power and authority to make final policy decisions. The Vice President of Information Technology is responsible for the development, maintenance, and publication of this policy.

VII. Procedures

A. Eligibility

All Sinclair faculty and staff are eligible for network accounts. Network accounts include access to Microsoft Outlook communications software for email and calendar services. If an account is required for an individual who is not a member of the faculty or staff, a letter from the Dean or Director of the affected department is required. The letter must state the purpose for granting access and for how long access will be needed. Access will be granted after approval by the I.T. Security Team.

B. Network Account Access

1. Network Access is issued automatically to all Sinclair faculty or staff after they have been entered into the Human Resources system (Colleague database).
2. Employee status is validated by determining if a user has received a check within the last six months. If they have received a check within the last six months and their employment has not been explicitly terminated, an account may be created.
3. These network accounts provide access to email, calendaring, and scheduling systems, and to the campus network. The accounts also provide access to Sinclair's internal Intranet site, <http://intranet.sinclair.edu>, as well as the external "public" web site, <http://www.sinclair.edu>.
4. The login ID (also called user name) format is: **firstname.lastname**
5. The email address format is: **firstname.lastname@sinclair.edu**
6. Account information for Network access can be obtained by:
 - a. Accessing new account information from both on and off-campus from any Internet connected computer through using Microsoft Outlook Web Access.

SEE also Outlook Web Access

- b. The **initial password** is: **PassXXXX** (the word Pass followed by the last 4 numbers of the user's social security number). Please remember that passwords are case sensitive.
- c. Security is important. A user should set up a shared secret and change the default password immediately upon accessing the account. A "Password Assistant" wizard is available on the Intranet main page to guide users through this process.

See also Outlook Web Access

See also the Password Assistant Icon on the Sinclair Intranet Page

7. Users can also go to the Help Desk with their Tartan Card for help with accessing their new accounts.

Glossary

Anti-virus Software

Programs to detect and remove computer viruses. The simplest kind scans executable files and boot blocks for a list of known viruses. Others are constantly active, attempting to detect the actions of general classes of viruses. Anti-virus software must be regularly updated to be effective against the latest viruses as they are released and discovered.

Chain Letter

Any message that is unrelated to the mission of the College that has been forwarded more than 10 times is, by our definition, a chain letter.

Colleague Application/Database

The application (developed by Datatel, Inc.) used by the College for Enterprise Resource Planning (ERP). It is a collection of software programs that tie all of the various diverse functions (student services, business operations, finance, HR, etc.) into a cohesive database.

College Email System or Services

Electronic mail system or services owned or operated by Sinclair Community College or any of its divisions.

Electronic Mail Services/System

Any messaging system that depends on computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records for purposes of asynchronous communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic mail; or is implicitly used for such purposes, including services such as electronic bulletin boards, listserves, and newsgroups.

Electronic Mailbox

A file (or folder) designated to a particular user on a particular computer in which received electronic mail messages are stored ready for the user to read them. Using the example `firstname.lastname@sinclair.edu`, "firstname.lastname" is the name of the user's mailbox file on the mail server.

Email Address

The string used to specify the source or destination of an electronic mail message. A typical college e-mail address format is `firstname.lastname@sinclair.edu`

Email Distribution List

A distribution list is a group of recipients, all gathered under one name, or address. A distribution list allows you to send a message to all of the recipients by entering just that one address. There are two common kinds of distribution lists: Personal Distribution Lists (PDL) and Server-Based Distribution Lists (SDL). See their individual definitions.

Email Record/Email Message

Any or several electronic computer records or messages created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several email systems or services. This definition of email records applies equally to the contents of such records and to transactional information associated with such records, such as headers, summaries, addresses, and addressees. This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail.

Email Users

Individual(s) who create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print email (with the aid of College email services). A (College) Email User is an individual who makes use of (College) email services. Receipt of email prior to actual viewing is excluded from this definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the email record.

Encrypted/Encryption

Procedures using algorithms to encode or convert plain text into ciphertext to prevent any but the intended recipient from reading that data. There are many types of data encryption; they are the basis of network security.

Holder of an Email Record or Email Holder

An email user who is in possession of a particular email record, regardless of whether that email user is the original creator or a recipient of the content of the record.

Letter or Mail Bomb

An e-mail message containing malicious code intended to do nefarious things to the recipient's computer or network. Also, to send, or urge others to send, massive amounts of electronic mail to a single system or person, with intent to crash or spam the recipient's system. Letter or Mail bombing is a serious offense and is not tolerated.

List Owner

Individual(s) who establish the scope and distribution of and perform the maintenance of email distribution lists.

Malicious Code

Code is a common term used to describe a set of instructions to a computer, also called program or software. Malicious code in general can be defined as "software which interferes with the normal operation of a computer system." Another general definition might be "software which executes without the express consent of the user." Common types of malicious code include viruses, Trojans, and worms.

Microsoft Outlook

The Microsoft "groupware" information management and communication software used by the college for e-mail communication, group planning and scheduling, and contact/task management.

Personal Distribution Lists (PDL)

These are created by individuals for their individual use. Personal distribution list files are stored on the individual's Personal Address Book. Personal Address Books usually reside on the individual's hard drive (or a drive of their choice). These lists are called "Personal" as they should be created for personal (one person) use. Sinclair users are permitted to create and share PDLs to facilitate group communication.

Server

A computer that provides some service for other computers connected to it via a network. A mail server has a drive that hosts user's electronic mailbox and receives, stores, and sends e-mail messages via the network.

Server-Based Distribution Lists (SDL)

These are created by ITS for use by multiple users. The distribution list files are stored on the Exchange Mail server. These lists are called "Server Based" as they are designed to be used by more than one person. Use of these lists is restricted for authorized purposes only as misuse wastes system resources and can effect the entire College network.

Spam or Spamming

Electronic junk mail or junk newsgroup postings. Spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. Spamming is sending or transmitting these junk messages. Receipt of Spam is virtually impossible to control; Spamming to or from college e-mail systems is strictly prohibited.

Use of College or other Email Services

To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print email (with the aid of College email services). A (College) Email User is an individual who makes use of (College) email services. Receipt of email prior to actual viewing is excluded from this definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the email record.

User/Login/Logon ID

The string that, in conjunction with the password, identifies a user to the network. A typical college user ID consists of the user's first and last name separated by a period. as in "firstname.lastname".

Virus

A program or piece of code that generally executes without the user's knowledge and runs against their wishes. Most viruses are malicious in nature and can also replicate themselves. All computer viruses are manmade and vary in degree of danger. Even a simple virus that replicates itself without actually harming system files is dangerous because it quickly uses available memory and other resources. More dangerous types of virus are is one capable of transmitting across networks and mutating to bypass security systems.

Index

A

Access 7

Account Responsibility 4

All Sinclair Mail Users 5

Archiving and Records Retention 8

C

Chain Letters 6

College Property 4

Confidentiality 6

D

Disclosure 7

E

Email Address Formats 4, 9

Email Distribution Lists 5

Employee Network Files 7

 Supervisor Access 7

F

Firstname.lastname@sinclair.edu 4

H

Help Desk 4, 7, 9

Human Resources 4, 9

I

Information Technology 8

 Vice President 8

Interference 6

Intranet.sinclair.edu 9

Introduction 3

L

Letter Bombs 6

M

Mailbox Space Limits 4

Microsoft Exchange 4

 limit 4

Microsoft Outlook 9

Microsoft Outlook Web Access 9

N

Network Access 4, 9

Network Account Access 9

P

Password Assistant..... 9
Policy Responsibility..... 8
Policy Statement Purpose..... 4
Policy Violations and Sanctions..... 8
President’s Bulletin..... 5
Procedures..... 9
Purpose..... 3

R

Restrictions..... 5
Records Retention..... 8
Representation..... 5

S

Scope..... 3
Security..... 7
Security Team..... 9
Sniff..... 7
Spam..... 6
Special email addresses..... 4
Specific Restrictions..... 5
Spoofing..... 6
Supervisor Access..... 7
 Employee Network Files..... 7

T

Tartan Card..... 9

U

Users..... 4

V

Vice President..... 8
 Information Technology..... 8

W

Web Access..... 9
www.sinclair.edu..... 9