



SUBJECT	E-MAIL POLICY
<p>Purpose</p> <p>This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.</p> <p>Scope</p> <p>The policies apply to Northern College (NC) employees and covers e-mail located on NC personal computers and servers if these systems are under the jurisdiction and/or ownership of NC. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.</p> <p>Policy</p> <p>1. College Property</p> <p>As a productivity enhancement tool, Northern College encourages the use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Northern College, and are not the property of users of the electronic communications services.</p> <p>2. Authorized Usage</p> <p>Northern College electronic communications systems generally must be used only for College activities. Incidental personal use is permissible so long as:</p> <ul style="list-style-type: none"> (a) It does not disrupt College resources (b) It does not interfere with staff productivity. (c) It does not preempt any business activity. <p>Users are forbidden from using Northern College electronic communications systems for charitable endeavors unless expressly approved by their supervisor and the Manager of Information Technology. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use</p> <p>3. Default Privileges</p> <p>Employee privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software.</p> <p>4. User Separation</p> <p>These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. All Northern College staff have unique usernames and passwords to access the e-mail system.</p>	

SUPERSEDES	REFERENCE	ISSUE DATE	SECTION	PAGE OF	
		April 13/04		1	6



SUBJECT	E-MAIL POLICY
----------------	----------------------

5. User Accountability

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password. If users need to share computer resident data, they should utilize message-forwarding facilities, public folders on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities).

6. No Default Protection

Employees are reminded that Northern College electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. Contact the IT department if this requirement is needed.

7. Respecting Privacy Rights

Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. Northern College is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, Northern College has a responsibility for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications when it is suspected that the College’s e-mail system is being used inappropriately. Some examples are:

- Forging, or attempt to forge, electronic mail messages.
- Attempt to read, delete, copy, or modify the electronic mail directed to other users without prior consent.
- Sending, or attempt to send harassing, obscene and/or other threatening email to another user.
- Sending unsolicited “for-profit” messages or chain letters.
- Sending unauthorized network broadcast messages

SUPERSEDES	REFERENCE	ISSUE DATE	SECTION	PAGE OF	
		April 13/04		2	6



SUBJECT	E-MAIL POLICY
	<p>printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.</p> <p>9. Regular Message Monitoring</p> <p>It is the policy of Northern College NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that NC will from time to time examine the content of electronic communications. Monitoring is only undertaken with the approval of the employee’s supervisor and the Manager of Information Technologies and Properties. The employee may or may not be made aware of such monitoring depending upon the nature of the request.</p> <p>10. Statistical Data</p> <p>Consistent with generally accepted business practice, Northern College collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone-switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Information Technology (IT) staff monitor the use of electronic communications to ensure the ongoing availability and reliability of these systems.</p> <p>11. Incidental Disclosure</p> <p>It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the request of individuals who have not received approval from the Human Resources Department.</p> <p>12. Message Forwarding</p> <p>Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Northern College sensitive information must not be forwarded to any party outside Northern College without the prior approval of their supervisor. Blanket forwarding of messages to parties outside Northern College is prohibited unless the prior permission has been obtained.</p> <p>13. Purging Electronic Messages</p> <p>Users, from their personal electronic message storage areas, should periodically purge messages. Not only will this increase scarce storage space; it will also simplify record management and related activities. If Northern College is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the Northern College President, or his designated representative, has communicated that it is legal to do so.</p>

SUPERSEDES	REFERENCE	ISSUE DATE	SECTION	PAGE OF	
		April 13/04		3	6



SUBJECT	E-MAIL POLICY
<p>14. Responsibilities</p> <p>As defined below, Northern College groups and staff members responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility.</p> <p>14.1 Information Technology must establish e-mail security policies and standards and provide technical guidance on e-mail security to all Northern College staff.</p> <p>14.2 IT staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their staffs are in compliance with the personal computer security policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to e-mail security.</p> <p>14.3 Northern College managers must ensure that employees under their supervision implement e-mail security measures as defined in this document.</p> <p>15. Disciplinary Process</p> <p>Violation of these policies may subject employees to disciplinary procedures up to and including termination.</p> <p style="text-align: center;">Please refer to Appendix A for “E-mail Best Practices”</p>	

SUPERSEDES	REFERENCE	ISSUE DATE	SECTION	PAGE OF	
		April 13/04		4	6



INFORMATION TECHNOLOGY

SUPERSEDES	REFERENCE	ISSUE DATE	SECTION	PAGE OF
		April 13/04		5 6



Format

The format or layout of your e-mail serves to maximize readability.

Use numbers and bullets to recap or list agenda and action items.

Write a series of brief paragraphs, and always insert a line between them.

Avoid all-caps – it comes across as shouting. If you need emphasis, put asterisks on either end of the word or phrase. Conversely, avoid typing in all lower-case.

Style

Style is the hardest element to master. Too rigid, and you could come off as humorless and intimidating. Too casual, and you may be dismissed as someone not to be taken seriously.

Know your audience. This will dictate the level of formality required. A “business casual” tone will suit most occasions. Think “khakis and a golf shirt.”

Avoid acronyms like TIA (thanks in advance) or BTW (by the way). A lot of people will have no idea what these mean.

Avoid making jokes – they often misfire.

Responding

E-mail communication is a two-way street. Responding to e-mail in a professional manner is just as important as being a good e-mail writer.

Don't reply unless it is required in some way

Respond to e-mail messages promptly. If you need more time, send a brief acknowledgement telling the sender when you'll respond in full.

Always refer back to the content in the sender's original e-mail. Quote them.

Consider “interweaving” your response within the sender's original text, especially if they want feedback on multiple issues. This makes it clear what item you are addressing in your response.

SUPERSEDES	REFERENCE	ISSUE DATE	SECTION	PAGE OF	
		April 13/04		6	6