NORTHEAST COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE NUMBER: AP-3511.5

ELECTRONIC MESSAGING

1. PROCEDURE SUMMARY STATEMENT

To establish protocols on creating, sending, receiving, storing, preserving, or otherwise processing information by electronic messaging.

2. DEFINITIONS

2.1 Record – The Records Management Act (Revised Statutes of Nebraska, Chapter 84, Article 12) defines a record as: "any book, document, paper, photograph, microfilm, sound recording, magnetic storage medium, optical storage medium, or other material regardless of physical form or characteristics created or received pursuant to law, charter, or ordinance or in connection with any other activity relating to or having an effect upon the transaction of public business." A record is information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

2.2 Public Record – The Records Management Act (Revised Statutes of Nebraska, Chapter 84, Article 12) defines a public record as follows: "Public records includes all records and documents, regardless of physical form, of or belonging to this state or any agency, branch, department, board, bureau, commission, council, subunit, or committee of this state except when any other statute expressly provides that particular information or records shall not be made public. Data which is a public record in its original form shall remain a public record when maintained in computer files."

2.3 Electronic Record – A record created, generated, sent, communicated, received, or stored by electronic means.

2.4 Electronic Message – Any communication using an electronic system for the conduct of official business internally with employees, students, and others outside the College. These messages may be in the form of email, text, instant messaging, electronic document exchange (electronic fax), voice mail, and electronic data interchange (EDI).

2.5 Electronic Mail (Email) – A system that enables users to compose, transmit, receive, and manage text and/or graphic electronic messages and images across networks and through gateways connecting other local area networks. This information consists primarily of messages, but may include attachments such as calendars, directories, distribution lists, word processing documents, spreadsheets, and other electronic documents.

3. PROCEDURE

3.1 Usage

3.1.1 Technology Services will assign an official College email address to all students, faculty, and staff. It is to this official address that the College will send email communications. Employee email addresses will be the listed in the Global Address Book for the College's email system. Email accounts will be granted to third party non-employees on a case-by-case basis.

3.1.2 Users do not own their email accounts provided to them by the College but are granted the privilege of exclusive use. The College does not intend to act as a censor of information but reserves the right to inspect files or email and take appropriate action without notification if there is reasonable belief that there has been intentional or inadvertent disruption to the College's network or other shared resources or if there is suspected violation of College policies, procedures, or applicable laws. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, they must be aware of how to unsubscribe from the list and is responsible for doing so if their current email address changes. Email users are expected to remember that email sent from the College's email accounts reflects on the College and should comply with normal standards of professional and personal courtesy and conduct.

3.1.3 Manually forwarding College email that contains information classified as legally restricted or sensitive is only permissible for valid business purposes, and appropriate security precautions such as email encryption must be taken. Automation tools such as auto-forwarding, POP, IMAP etc., to move email from a College-managed email system is prohibited unless approved on a case-by-case basis for legal, personnel, or administrative purposes.

3.1.4 Email access will be terminated when the employee or third party terminates their association with College unless other arrangements have been approved. Student email access will be terminated at the end of their active enrollment period. The College is under no obligation to store or forward the contents of an individual's email mailbox after the term of employment or enrollment has ceased.

3.2 Record Classification

3.2.1 Electronic messages, in and of themselves, are not a single record series. The electronic messaging system is a means of transmitting messages. Electronic messages transmitted through a College system are records and as such are subject to management under the Records Management Act. Records

communicated using electronic communications need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research, or other requirements.

3.2.2 Electronic messages sent and received by users fall within two (2) broad categories: (1) transitory messages, including copies posted to several persons and casual and routine communications similar to telephone conversations; and (2) records with a permanent retention period. An electronic recordkeeping system should be able to separate messages into these two (2) categories.

3.3 Retention and Disposition

3.3.1 There is no single retention period for all electronic messages. Retention and disposition of electronic messages depends on the function and content of the individual message. Thus, a universal rule that all electronic messages will be deleted after a defined period is not a comprehensive solution to managing electronic messages. The various types of electronic messages require various retention periods – whether of a long-term or more ephemeral nature.

3.3.2 The end-user manages electronic messages. Electronic messages should be managed at the end-user's email client rather than from a central point. Each end-user is responsible for managing records that are part of their electronic messaging system.

3.3.3 Transitory electronic messages that have no administrative legal, fiscal, or archival retention requirements may be deleted as soon as the messages have served their purpose. Such records include, but are not limited to, the following:

3.3.3.1 Information-only copies, or extracts of documents distributed for reference or convenience, i.e., announcements or bulletins;

3.3.3.2 Copies of published materials;

3.3.3.3 Telephone message notifications;

3.3.3.4 Preliminary drafts unless a retention period is otherwise specified on an applicable records retention schedule; and

3.3.3.5 Reservations and confirmations.

3.3.4 Emails sent or received which has lasting operational, legal, fiscal, or historical value to the College’s programs, administration, or operations should be retained in accordance with the College’s Record Management Policy (BP-3070). These messages must be transferred to another medium and filed with the custodian of record, permitting email records to be purged at regular intervals from campus servers or daily from trash folders in email applications.

Information system administrators routinely backup servers, and the backup media are recycled on a timetable. It is important not to rely upon this backup exclusively for electronic messages. If non-transitory electronic messages are to be filed electronically, information system managers should be consulted.

3.3.5 All electronic messages should be disposed of in a manner that ensures protection of any sensitive, proprietary, or confidential information. Magnetic recording media previously used for electronic records containing sensitive, proprietary, or confidential information should not be reused if the previously recorded information can be compromised in any way by reuse.

3.4 Access

3.4.1 Requests for access to non-confidential electronic messages should be treated in the same manner as requests for other public records. The difficulty of retrieval is not a legitimate reason to deny access. Throughout the retention period, electronic messages should remain reasonably accessible.

3.4.2 Prior to any inspection, monitoring, or disclosure of the contents of College electronic communication records in a user's possession, the user's consent shall be obtained except as provided for below:

3.4.2.1 When required by and consistent with law;

3.4.2.2 When there is substantiated reason to believe that violations of law or of College policies or procedures have taken place;

3.4.2.3 When there are compelling circumstances; or

3.4.2.4 Under time-dependent, critical operational circumstances.

3.5 Litigation

3.5.1 When litigation against the College or its employees is filed or threatened, the law imposes a duty upon the College to preserve all documents and records that pertain to the issue(s). When the College’s Legal Counsel is made aware of pending or threatened litigation, a litigation hold directive will be issued to the custodian of record and appropriate technology staff for coordination of storage and retention.

3.5.2 A litigation hold directive overrides this procedure, as well as any records retention schedules that may have otherwise called for the transfer, disposal, or destruction of relevant documents, until the hold has been cleared by the College’s Legal Counsel.

3.5.3 College business-related electronic messages stored on non-College computers or within non-College accounts may be subject to public records

requests, legal discovery, court-ordered production, audit review, and records retention requirements.

3.6 Backups

3.6.1 Backups of email systems are for business continuity or disaster recovery only and are not kept for record keeping purposes. Technical staff should be physically expunging and/or purging backup media, and this should happen in compliance with a routine schedule. Backup Medias are designed to recover a system in the event of a catastrophe or incident that renders data irretrievable, and when a new backup is run, the earlier ones should be overwritten, destroyed, or otherwise rendered unusable.

3.7 Technical Security and Limitations

3.7.1 The technical staff at the College reserve the right to:

3.7.1.1 Set the amount of space available for electronic communications mailboxes;

3.7.1.2 Limit the size of email attachments transferred by the College's mail servers. The current limit is 25MB;

3.7.1.3 Carry out necessary purges of information stored on the servers to preserve the integrity of the system; and

3.7.1.4 Run virus scans and quarantine electronic communications that contain viruses.

3.8 Text Messaging

3.8.1 The College will use text messaging to enhance communication with alumni, donors, students and employees for emergency warnings or safety notifications, authorized student success initiatives and pre-approved limited promotional messages. Individual text messages sent for the purposes of student success shall be professional, individually targeted messages that communicate such items as routine business needs, upcoming deadlines, or appointment reminders. Text messages may not include private information protected under the Data Protection Plan and shall not release any identifiable information protected under FERPA. System generated group text messages shall (1) include an option for the recipient to opt-in/opt-out of receiving text messages, (2) be accessible for all intended recipients, and (3) be professional and not include text abbreviations. Approved departments can use mass text messaging to effectively communicate while being a good steward of information, respecting the privacy and wishes of the recipients, and adhering to applicable state and federal laws. Northeast may use text messaging to complement existing forms of communication such as letters, email, social

networking sites and the Northeast website. Mass text messaging must support other forms of communication and not be the primary means of communication.

3.8.2 The Vice President of Student Services may work with College divisions or departments to adopt an annual plan that details the purpose, content, frequency and audiences of text messages. The identified publisher of text messages in the respective divisional or departmental plan shall be authorized to send text messages pursuant to such plan. All other non-emergency text communications shall be approved by the Vice President of Student Services, or their designee, prior to being sent.

3.8.3 The Vice President of Student Services shall adopt a Terms and Conditions document with information for individuals to opt-in and opt-out of receiving text messages. Such document shall a) include a statement that message and data rates may apply depending upon the service carrier provider; and b) provide individuals with contact information for assistance.

3.9 Instant Messaging, Chat, and Collaboration Tools

3.9.1 Individuals who use resources such as forums or newsgroups, instant messaging, email lists, chat services, collaboration tools, etc. shall decide for themselves whether the forum and content are appropriate to their needs. The College will treat these services as an educational resource. Transmission of information by electronic means does not negate intellectual property rights, copyrights, or other protections. At College management discretion, files, data, or communications may be reviewed as necessary; therefore, individuals are not entitled to any expectation of privacy regarding their files, data, or communication.

3.9.2 The content of any message sent through the any electronics messaging system is the sole responsibility of the individual sending the message and should follow the Acceptable Use Procedures – Technology Resources (AP-3511.1). Harassment, obscenity, forgery, and other illegal forms of expression are not acceptable use of university resources. The only enforceable restrictions on content of electronic messages are those that apply generally to verbal or written communication (slander, harassment, SPAM, etc.). When such restrictions need to be enforced, the same administrative, judicial, and criminal processes as for non-computer communication may be invoked. Use of electronic messaging systems does not change what is and is not an illegal communication. The College will not censor or regulate messages based on content or views expressed by the sender or implied by the receipt.

4. APPLICABILITY

N/A

ISSUE DATE: 08/10/2022
EFFECTIVE DATE: 08/10/2022
REVISION DATE(S): 08/10/2022
PRIOR POLICY/PROCEDURE NUMBER: none
SCHEDULE FOR REVIEW: 2027
DIVISIONS/DEPARTMENT RESPONSIBLE FOR REVIEW & UPDATE: Technology Services
SPONSORING DIVISION/DEPARTMENT: Technology Services
RELATED PROCEDURES/ REFERENCE: AP-3511.0, AP3511.1, AP-3511.2, AP3511.3, AP3511.4, AP-3070.0
PROCEDURE KEY WORDS: email; chat; electronic messaging