Information Technology – Electronic Mail Policy

Electronic Mail (email) is a tool provided by Bellin College to complement traditional methods of communications and to improve academic and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical, and lawful manner. Use of the College email system implies consent to all College IT policies and practices. Violations of the policy may result in restriction of access to the College email system and/or other appropriate disciplinary action.

Senior students who graduate will have their Bellin College email account transitioned to an alumni email account two weeks after graduation. Instructions will be sent prior to the transition.

Scope

This policy applies to all users of Bellin College technology resources. A "user" is defined as any individual who logs into, uses, or attempts to log into or use a College system; or any individual who connects to, or attempts to connect to or traverse the College network, whether by hardware or software or both, whether on campus or from a remote location.

Policy

The Bellin College Microsoft Exchange email system is the only recognized email system used to communicate between faculty, staff, and students. This is necessary to ensure the delivery and receipt of official communications. Email messages regarding College matters sent from an administrative office, faculty or staff member to students is considered to be an official notice and should be treated as such by the student.

Acceptable Use

Reference the Acceptable Use Policy for guidance on acceptable use, inappropriate use, and user responsibilities. Users must exercise caution when forwarding messages, either internally or externally. Sensitive information - such as social security numbers, addresses, age, gender, etc. - must not be forwarded to any party outside of the College without the prior knowledge or approval of that individual.

User Responsibility

Users are expected to read email on a regular basis and manage their accounts appropriately.

Sharing passwords is strictly prohibited. Each user is responsible their account, including safeguarding access to the account. All email originating from an account is deemed to be authored by the account owner and it is the responsibility of that owner to ensure compliance with these guidelines.

Privacy

Bellin College will make every attempt to keep email messages secure; however, privacy is not guaranteed, and users should have no general expectation of privacy in email messages sent through the College system. Users must be aware that email can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Email that is not encrypted can be viewed by people other than the intended recipient, while it is in transit or on mail servers. Because messages can be stored in backup systems, email may be retrievable when a traditional paper letter would have been discarded or destroyed.

Email Etiquette

When using email as an official means of communication, users should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, users should not communicate anything via email they would not be prepared to say publicly. The following practices should be followed when using email.

- Use a meaningful subject line when sending a message.
- Be concise.
- Use proper spelling, grammar, and punctuation.
- Avoid abbreviations that the reader may not be familiar with.
- Do not attach unnecessary files.
- Use proper layout and structure.
- Do not overuse the high priority option.
- Use upper and lower-case letters in your message. Messages typed in all upper case give the impression of shouting.
- Be selective about recipients. Use of distribution lists or ‘reply all’ features should be carefully considered and only used when necessary.
- Read the email before sending.
- Only use delivery and read receipts when necessary.

System Monitoring

Bellin College collects statistical data about its email systems consistent with generally accepted business practices. The College monitors the use of email to ensure the ongoing availability, reliability, and security of the system. The College may employ, at any time, tools to analyze statistical information to detect unauthorized usage, denial of service attacks, capacity planning and network problems. Under certain circumstances, it may be necessary for the IT staff or other appropriate College officials to access email files to maintain the system, to investigate security abuse incidents, and violations of this or other College policies. Such access will be on an as-needed basis and any email accessed will only be disclosed to those individuals.

Mailbox Size Limits

The Outlook mailbox quota is set at 2GB for all users, this includes the messages in your inbox, sent items and deleted items. The College has the right to restrict the amount of user space on the email server as necessary and to revise the size restrictions, as necessary.

Records Retention

Individuals are responsible for saving email messages as they deem appropriate. Messages are automatically purged from folders in order to save storage space. Automatic purge amounts are as follows:

- Sent - 365 days
- Deleted Items - 90 days

- Junk - 30 days

Inbox items are not automatically deleted. Individual users are responsible for deleting unneeded email in order to stay within their mailbox quota.

Email Size Limits

A 100-megabyte size restriction for all email is enforced whether being sent or received. This is necessary to preserve network bandwidth and mailbox storage resources.

Email Signature

Email signatures indicating name, job title, address, contact info and other particulars are strongly recommended for all email messages whether sent to internal or external receivers.

Data Backup

The email system is backed up on a nightly basis and stored for 30 days.

SPAM and Virus Protection

Bellin College utilizes SPAM filtering and anti-virus software. Virus-infected email often appears to be sent from a friend or coworker and will contain an attachment. This attachment is the virus carrier and, by opening the attachment, the virus code is executed. Attachments should be opened only when you are sure of the sender and message.

IT Services will make every effort to prevent these types of messages from entering our system. Contact the Helpdesk if any doubts exist; helpdesk@bellinCollege.edu; (920) 433-6666.