

Email System

Acceptable Use and Security Policy

POLICY:

Electronic messaging (Email) is an essential and enabling application that facilitates the flow of information within the College and with external correspondents. Electronic messaging systems will be managed and protected across the College in accordance with common standards and procedures.

Rationale:

The College depends on the availability and responsiveness of Email for the normal conduct of College business. The widespread acceptance of Email both within the College and as a part of our personal lives as a means of rapid communication and dissemination of information has led to the availability of a wide variety of consumer and enterprise applications and services. These applications and systems can be purchased and installed often without regard for the necessary ongoing administrative support needed to maintain system integrity and the security or confidentiality of the information conveyed by the system. For the conduct of College business using email, efficiency of operation and maintenance of security can best be achieved by limiting the number of Email systems serving the College and by using only enterprise class systems to supply email accounts.

Indiscriminate mass emailing to the College community can quickly tax the capabilities of the processing systems to deliver other messages that may be critical. Additionally, the receipt by College users of excessive numbers of mass emailing messages is a work-place irritant and does not promote the efficient use of information system or human resources.

Email does not include instant messaging (IM) capabilities.

Standards & Procedures:

Standards:

Attachment Type Limitations. Email attachments received on campus will be filtered to exclude specific filename extensions (e.g. .exe, .com) as may be determined to be a security threat by the College Information Security Officer.

Official Business Communications. All official Darton College business communications via email, must be sent through the Official Darton College email systems.

Conveyance of Confidential or Sensitive Information. Users of all Email systems must be aware that information originated in or received through email messages is probably not encrypted and should not be considered as confidential or unaltered. Unencrypted email will not be used for the conveyance of personal or sensitive information (see [Sensitive Information Protection Policy](#)).

Email Broadcasts. Use of the centrally managed Email systems of the College for mass distribution of mailings will be governed by the criticality of the content of mailings as follows:

Critical Messages. Critical messages that need to be distributed to all College employees must be approved by the President, a Vice President, the Director of College Relations, or the Chief Information Officer prior to submission for distribution. Critical messages intended for students must be approved by the Vice President for Student Services prior to distribution. Critical messages are categorized as either *time-sensitive* or *non-time-sensitive*.

Informational Messages. Users of email systems at Darton College are not permitted to arbitrarily send messages to all, or nearly all, of the system users unless they are Darton College business related. Instead, Luminis Groups have been created and are designed to reach targeted audiences. Individuals may selectively join any, or all, of these groups.

Email Relay. All College hosted email systems will be configured to prevent use by third parties as email relay platforms.

Email Systems. Office of Information Technology (OIT) will operate centrally managed email systems for the College to support the needs of faculty, staff, and students (and retirees as resources permit).

Passwords. Strong password guidelines as published in **Minimum Information Security Environment Policy** (Create or Change a Password) will be utilized on all College hosted Email systems.

Patch Management. Email servers must be updated with new security patches for both the operating system and mail server applications as those patches are released by vendors. OIT is responsible for patching the centrally managed email systems.

Student Email. All students registered for classes at Darton College are provided an email account through their access to the Darton College Campus Pipeline (MyDC) system. The College will use this email account to send communications to the student body. Student email addresses will be recorded in the College's electronic directories and records. Students are responsible for reading official College email in a timely fashion.

Virus Detection and Removal. Active anti-virus detection and quarantine clients will be installed on all email servers. Where possible, these anti-virus applications will be configured for automatic update of virus signatures. Additionally, anti-virus gateways will be utilized to scan inbound and outbound messages.