UNIVERSITY POLICY

Policy Title: Access to Large Distribution Email Lists

Policy Number: 4.5.0.0
Campus: ☐ Lisle ☐ Mesa ☒ Both
Policy Status: ☒ New policy ☐ Continuing/active policy ☐ Archive policy
Supersedes: not applicable

Policy Origination/Approval Date: 2/16/2026
Review Period: Annually
Last Revision Date: 2/16/2026
Last Review Date: 2/16/2026
Next Scheduled Review: 2/16/2027

Associated Division(s): Enrollment and Marketing
Responsible Office(s): Information Technology & Marketing/Communications
Name(s) of Designated Policy Owner(s): Nick Pluta & Kit Avanzado

Approved By:

- **University Planning Council Subcommittee on Policies:**
  Tim Marin, Ellen Ziliak 2/13/2026
- **President:**
  Joseph Foy 2/13/2026

---

1. Purpose

Benedictine University is committed to maintaining clear, consistent, and secure communication with our campus community. To streamline university-wide messaging and protect institutional data, this policy establishes guidelines for which faculty and staff members are authorized to send emails to large distribution lists, including all-faculty, all-staff, all-student, or all-campus lists.

2. Scope

This policy applies to all Benedictine University employees, including full-time and part-time faculty, staff, administrators, contractors, and student workers who may request or currently possess access to university-wide email distribution lists.

3. Definitions

- **Policy:** A formally approved statement that mandates or constrains actions to guide decision-making and ensure consistent institutional practice. Policies are binding on members of the University community.
- **Responsible Office:** Information Technology & Marketing/Communications
- **Policy Owner:** The senior administrator overseeing the Responsible Office who ensures that the policy aligns with University mission and compliance obligations.

4. Policy Statement

To ensure effective communication and maintain the security and integrity of university email systems, access to large distribution lists will be restricted to key individuals in roles deemed critical to institutional operations, safety, and compliance.

The University is currently reviewing all existing permissions and will retain access only for individuals whose job responsibilities require them to distribute information broadly on behalf of their department, division, or the University as a whole.

Faculty and staff who do not retain access must route any requested communication through their designated leadership as outlined below.

5. Authorized Users

Access to send messages to university-wide distribution lists will be provided only to the following:

- President's Cabinet Members
- Academic Deans and Dean of Students
- Department or Division Heads whose roles require cross-campus communication as approved by Cabinet
- Staff in Communications, Registrar, Enrollment, and other areas responsible for university-wide messaging
- Campus Safety and relevant emergency communication personnel
- Other individuals explicitly approved by the Office of Information Technology and University Leadership

A current roster of authorized senders will be maintained by the Office of Information Technology and Marketing/Communications.

6. Required Communication Channels for All other Faculty and Staff

Faculty and staff who are not authorized to use large distribution lists must route messages as follows:

- Faculty: Through their Dean or Dean's Office representative (e.g., Dean's Assistant)
- Staff: Through their Department Manager, Director, or Cabinet-level supervisor

These individuals will determine whether the message is appropriate for university-wide distribution and will coordinate with the appropriate offices as needed.

All University policies

7. Rationale

This policy is designed to:

- Streamline communications and reduce redundancy and message overload
- Maintain consistent, professional institutional messaging
- Enhance security by limiting the number of individuals with broad email sending capabilities
- Protect the integrity of university-wide communication channels

8. Compliance

Unauthorized use of large distribution lists may result in:

- Temporary or permanent removal of access
- Review by the employee's supervisor
- Other actions in accordance with University technology policies and HR guidelines