Policy # 56012

EMAIL USE POLICY

Effective Date: July 2006 **Reviewed Date:** January 1, 2022
Responsible Office: Information Technology Center
Division: Finance

I. PURPOSE/OBJECTIVE

The objectives of this policy are to outline appropriate and inappropriate use of Grambling State University's email systems and services in order to minimize disruptions to services and activities, as well as comply with the guidelines of the university's Electronic Communications Policy - #56006 and the Office of Information Technology (OIT) IT-POL 1-20.

II. STATEMENT OF POLICY

Email is a critical mechanism for business communications at Grambling State University. However, use of Grambling State University's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of Grambling State University.

This policy covers appropriate use of any email sent from a Grambling State University email address and applies to all employees, students, affiliated personnel, and agents operating on behalf of Grambling State University.

This policy also applies to all email systems and services owned by Grambling State University, all email account users/holders at Grambling State University (both temporary and permanent), and all company email records.

Important official communications are often delivered via email. As a result, employees of Grambling State University with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business- and role-oriented tasks.

Email users are also expected to comply with normal standards of professional and personal courtesy and conduct.

A. Definition

1. For purpose of this policy, the term "email" refers to the electronic transmission of information through a mail protocol such as SMTP or IMAP for communicating university business. A typical email client is Microsoft Outlook.

B. Email Access

1. All employees, students, and approved affiliated personnel of Grambling State University are entitled to an email account.

2. The faculty, staff, and approved affiliated personnel of Grambling State University are required to read and sign a copy of the Email Request Form prior to receiving an email access account and password.

3. Students currently enrolled or prospective students will receive email access.

4. It is the responsibility of the employee or student to protect the confidentiality of their account and password information. Strong passwords should be used and sharing of passwords is strictly prohibited. All email originating from an account is deemed to be authored by the account holder.

C. Special Email Accounts

1. Departmental Accounts/Student Organization Accounts

    a. Departmental accounts must be approved by the respective Vice President.

    b. Email accounts for student organizations must be requested and approved by faculty or staff.

    c. All departmental accounts/student organization accounts require a designation of an account holder who will manage the account including organization and cleaning.

    d. If no email is being sent from the departmental account/student organization account, the Information Technology Center (ITC) reserves the right to delete the departmental account/student organization account.

2. Affiliated Personnel

    a. Email accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include contractors and temporary guests.

D. Mailbox Quotas

1. Email accounts are assigned a disk quota on the email server which can only be increased based on a valid business justification.

E. Account Deletion

1. Faculty/Staff/Third Party

    a. Email access will be terminated when the employee or third party terminates their association with Grambling State University, unless other arrangements are made.

    b. Grambling State University is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased.

2. Students

    a. Email access will be terminated when the student is no longer enrolled at the university.

F. Mailbox Backup

1. Backup copies of email messages may exist, despite end-user deletion, for archiving of university records.

2. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss. In the event of a system disaster, email will be restored from the last backup.

G. Appropriate and Inappropriate Use

1. Using a reasonable amount of Grambling State University resources for personal emails is acceptable as long as it does not interfere with university operations or impact the faculty or staff's job performance.

2. The university's email accounts are scanned for incoming email that contain viruses, "SPAM" email, and unsolicited advertisements and are blocked from the user's inbox.

3. Unacceptable and inappropriate behavior includes, but is not limited to:

   a. Faculty/Staff/Third Party

      1. Forged Mail - It is a violation of this policy to forge an electronic mail signature or to make it appear as though it originated from a different person.
      2. Intimidation/Harassment - It is a violation of this policy to send/forward email that is obscene, harassing, abusive, or threatens an individual's safety. Known threats to personal safety will be reported to University Police.
      3. Unauthorized Access - It is a violation of this policy to attempt to gain access to another person's email files regardless of whether the access was successful or whether or not the messages accessed involved personal information.
      4. Unlawful Activities - It is a violation of this policy to send/forward copyrighted materials electronically, and it is a federal offense. Other illegal use of email will also be dealt with and/or reported to the proper authorities.
      5. Proprietary/Confidential Information - The unauthorized exchange of proprietary information or any other privileged, confidential sensitive information, without proper authorization, is a violation of this policy.
      6. Chain/Letters/Junk email/SPAM - It is a violation of this policy to send chain letters, junk email, or any other type of widespread distribution of unsolicited email.
      7. Hoaxes -It is a violation of this policy to distribute an email hoax with the intention to mislead or trick others into believing/accepting/doing something.
      8. Viruses -It is a violation of this policy to knowingly transmit email messages containing a computer virus, worm, spyware, or any form of malware.
      9. Commercial Activities - It is a violation of this policy to use Grambling's email system for commercial activities or personal gain.

   b. Student

      1. Forged Mail - It is a violation of this policy to forge an electronic mail signature or to make it appear as though it originated from a different person.

2. Intimidation/Harassment - It is a violation of this policy to send/forward email that is obscene, harassing, abusive, or threatens an individual's safety. Known threats to personal safety will be reported to University Police.
3. Unauthorized Access - It is a violation of this policy to attempt to gain access to another person's email files regardless of whether the access was successful or whether or not the messages accessed involved personal information.
4. Unlawful Activities - It is a violation of this policy to send/forward copyrighted materials electronically, and it is a federal offense. Other illegal use of email will also be dealt with and/or reported to the proper authorities.
5. Proprietary/Confidential Information - The unauthorized exchange of proprietary information or any other privileged, confidential sensitive information, without proper authorization, is a violation of this policy.
6. Junk email/SPAM - It is a violation of this policy to send junk email and SPAM email.
7. Hoaxes -It is a violation of this policy to distribute an email hoax with the intention to mislead or trick others into believing/accepting/doing something.
8. Viruses -It is a violation of this policy to knowingly transmit email messages containing a computer virus, worm, spyware, or any form of malware.
9. Commercial Activities - It is a violation of this policy to use Grambling's email system for non-student activities, commercial activities or personal gain.

H. Mass Email

1. All mass emails must be approved by the President, Media Relations or the Provost/Vice President for Academic Affairs.

I. Email Privacy

1. Grambling State University owns the data that is created, stored, and transmitted by the university. Therefore, the email systems and services are property of the university.

2. In the event of illegal use or malicious intent, Grambling State University has the right to monitor all email traffic passing through its email system.

3. While the university does not actively read end-user email, the university cannot assure the privacy of email messages.

4. If Grambling State University discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, email records may be retrieved and used to document the activity in accordance with due process.

J. Enforcement

1. The ITC will be responsible for reporting any breaches of this policy to the respective Vice President and reporting authority which may include disciplinary action.

III. REVISION/REVISED HISTORY

August 2011-Revision
July 2006-Effective Date