POLICY:

Georgia Perimeter College will provide all faculty, staff, and authorized third party users with accounts on the GPC email system and all messages sent by GPC will constitute an official means of communication.

PROCEDURE:

1. The college considers faculty and staff to be duly informed and in receipt of communications sent to their respective accounts via the GPC email system.
2. The GPC email system is the preferred mechanism for communicating with students for official academically related correspondence. However, apply these additional guidelines when communicating with students via email:
   - It is permissible to utilize other email systems which are an integrated component of vendor software solutions used by the college.
   - It is permissible to send general announcements regarding events to students’ third-party email accounts such as Hotmail and Yahoo.
   - GPC employees shall never send official academic-related correspondence to students using the employee's personal third-party email accounts such as Hotmail, Yahoo mail, etc.
3. Restricted information will not be sent via faculty and staff email to internal and external email addresses. OIT will determine the best method of sending restricted information. Restricted information includes those items spelled out in Information Security Policy 606, “Data Classification and Handling Policy”, under the section “Sensitivity Classification, III. Restricted Information”.
4. Faculty and staff employees must maintain password security and manage allotted storage space and data retention periods.
5. All academic units, student services units, or other institutional units that plan to use the email system to contact a subset of students must first develop policies to screen and to approve the message to ensure that only messages strictly related to official college or academic or service unit business are distributed.
6. Expiration of accounts:
   a. Email accounts for faculty and staff employees retiring from the college will be maintained indefinitely. This benefit ceases when the retiree is deceased.
   b. Email accounts for faculty and staff employees leaving the college on good terms will expire ninety days after the last day of employment.
   c. Email accounts for faculty and staff dismissed from the college will expire immediately upon termination
7. In addition to this policy, Policy 507 Appropriate Use of IT Resources also applies to faculty, staff, and third party use of the college email system.
8. Email account holders may not, under any circumstance, use “spoofing” techniques to disguise or masquerade their identities in sending email. Misrepresenting, masquerading, obscuring, suppressing,
or replacing an account holder’s identity on an email system for malicious or misleading purposes is prohibited.

9. Personnel may not view the content of another person’s email or grant access to this email at the request of other individuals, except in cases specifically authorized by the college administration. The contents of electronic mail will not be monitored, censored, or otherwise examined without specific authorization and direction by the executive vice president or the president of the college, with the following exceptions:

   a. Court order or law enforcement investigation may require the examination and release of any document, including electronic files such as email.

   b. Technical staff within the Office of Information Technology may monitor the use of email to ensure the ongoing availability, reliability, and security of the system. Statistical information collected will be used to detect unauthorized usage, denial of service attacks, capacity planning, and other infrastructure purposes. In the process of administering the electronic mail system, certain members of the OIT staff may have access to the contents of some email messages. The OIT staff will exercise their ability to access the contents of email under the strict limitations of the system administration requirements.

   c. A special condition exists for a staff employee who receives mail associated with his/her job responsibilities and where, in his/her absence, the supervisor of the department may need to have access to the mail. OIT must continue to maintain the privacy of mail, but on authorization from the department head, may locate and copy specific messages to facilitate departmental functions. No person outside of OIT may review the contents of an account's system mailbox without authorization of the executive vice president.

   d. Mail moved by the account holder outside the mail systems becomes a part of personal files covered by other policies and procedures.

10. OIT will enable and support the faculty and staff email system. Faculty and staff emails will be managed and protected across the college in accordance with common standards and procedures. Persons in violation of this policy are subject to a range of sanctions, determined and enforced by GPC management, including the loss of computer network access privileges, disciplinary action, dismissal from the college, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws. The college will carry out its responsibility to report such violations to the appropriate authorities.