Email Service Requirements

Purpose:

This Service Requirement defines the appropriate use of email for transmitting electronic messages using Duquesne University email systems. There is a reliance on electronic communications and email provides a fast, convenient, and cost-effective platform to deliver communications. It is imperative that Duquesne University provide an official form of e-mail as a means to communicate with our community members. This applies to all faculty, staff, consultants, students, retirees, and other authorized users that transmit and/or receive electronic messages using a Duquesne University email system.

These service requirements apply to any system or service that sends or receives electronic communications on behalf of Duquesne University. This includes but is not limited to: Office365 Email Service, Lyris Mailing Lists, Third-Party Contracted Services, and Mass Mailing Systems. As it relates to this service requirement, the term “technology environment” means any and all forms of information technology including computer-related equipment, software, accounts, tools, and intellectual property.

Service Requirements:
The Email Service Requirements specify the fundamental requirements for the appropriate use of email at Duquesne University. The fundamental email requirements cover:

1. Email as an Official Means of Communication
2. Email and Restricted Data
3. Email Accounts and Directory Information
4. Abuse of Email
5. Departmental/Group Accounts
6. Email Management and Administration

Service Requirements Specifications:

1. Email as an Official Means of Communication

A Duquesne University email account is an official method of communication for Duquesne
University administrative matters. A communication will be considered delivered one day following the date the communication is processed and delivered by your Duquesne University email account. Failure to check your email account does not excuse or exempt you from any actions required of you by the University. Communications regarding academic matters should be generated from an appropriate Duquesne University email account (domain duq.edu). It is not acceptable to utilize third party public or commercial email services (such as Gmail, Yahoo, Comcast, etc.) to facilitate email communications for academic purposes. This includes but is not limited to forwarding duq.edu email to an external mail service.

Duquesne University expects all full and part-time students registered in a degree program, and its faculty, administrators, and staff to activate and actively maintain a Duquesne University email account in order to receive University Communications. Individuals may opt to forward their Duquesne University email messages to another email account (e.g. @gmail or @outlook), but do so at their own risk. The University cannot guarantee the proper handling of email by outside services, third parties, or departmental email servers. Forwarding of email does not absolve an individual of the responsibilities associated with communication sent to official Duquesne University email addresses (MultiPassID@duq.edu).

Definition of “Technology Environment” for Duquesne University Email Service Requirement:

The technology environment is property of Duquesne University and as such retains exclusive rights to the environment including permission to monitor and log activity. All messages, data files and programs stored in or transmitted via the technology environment (“Electronic Communications”) are Duquesne University records. The University reserves the right to access and disclose all messages, data files and programs sent over or stored in its technology environment for any purpose. Duquesne University reserves the right to periodically examine any aspect of the technology environment and any other rights necessary to protect the technology environment.

2. Email and Restricted Data

Duquesne University email services are provided by Microsoft Office 365, which offers a level of privacy for Duquesne University higher than the public offering. However, email is not a secure mechanism for sharing data. Therefore, Restricted Data as defined in the CTS Data Governance Service Requirements is strictly prohibited from being sent in email. As stated in the CTS Data Governance Service Requirement this includes information that is regulated such as Personally Identifiable Information (PII), Family Educational Rights & Privacy Act (FERPA), Health Insurance Portability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA, the EU General Data Protection Regulation (GDPR) or other regulated data as defined. If restricted data is sent via email, the body of the message or attachment must be fully encrypted.

3. Email Accounts and Directory Information

Duquesne University individual and group email accounts are assigned by Computing and Technology Services (CTS) in order to send electronic communications. Accounts are assigned based on either your MultiPass ID or your group’s official University Name.

An individual’s email address is published in the Duquesne University directory (for students based on FERPA designation).
4. **Abuse of Email**

Use of email is a privilege, not a right. This privilege can be revoked and individuals can be subject to disciplinary or legal actions for inappropriate or unacceptable behavior included but not limited to:

- Sending unsolicited or unauthorized mass email (spam)
- Use of offensive language
- Distribution of obscene materials
- Threats
- Infringement on other’s privacy
- Interference with others’ work
- Copyright infringement
- Illegal activity
- Violates, or encourages the violation of, the legal rights of others or federal and state laws
- Alters, disables, or interferes with the use and operation of email services
- Misrepresents the identity of the sender of the email
- Creates a risk to safety or health, compromises national security, or interferes with an investigation by law enforcement
- Tests or reverse-engineers the email services in order to find limitations, vulnerabilities, or to evade filtering capabilities
- Spreads or distributes software that covertly gathers or transmits data about an individual

5. **Departmental/Group Accounts**

Departmental/Group accounts can be requested but will require a designation of a sponsor, who will administer the addition, deletion, or modification of individuals who are permitted to access the email mailbox. Group names have to represent an official organization, center, or initiative approved by the University Cabinet and/or Board of Directors.

6. **Email Management and Administration**

Duquesne University’s Computing and Technology Services (CTS) manages and administers the Microsoft Office 365 email solution.

- **Email Quotas and File Size Restrictions**

  As determined by Microsoft, email on the hosted Microsoft Office 365 system has a maximum file size for attachments of 35MB and a maximum mailbox size (including folders and deleted mail of 50GB).

- **Use of .pst folders.**

  The University strongly discourages the use of .pst folders for the archiving and storing of email messages. .pst folders are rarely backed up which can lead to data loss. Also, .pst’s are prone to corruption and only work on Outlook email clients. There also may be compliance issues if the .pst files are lost, stolen, or mishandled. If a .pst is required and used, CTS recommends that a password be placed on the file for security and privacy.
c. Legal Holds

Users who receive a legal hold from Legal Affairs are responsible for keeping copies of all relevant documents, including email. CTS also places legal holds within Microsoft Office 365 upon notification from Legal Affairs or from Human Resources.

d. Email De-Activation and Retention

The de-activation process for email accounts differ depending on the user's role at the University. That role along with the de-activation timeline determines how long email is retained for individuals.

a. Employees: Administrators/Staff/ Faculty
   i. Email is disabled immediately upon separation/last day worked. If such separation is for cause, email privileges may be immediately revoked without notice.
   ii. Email is retained for 60 days after last day worked and then deleted.
   iii. The University does not provide the forwarding of email from a former employee to a current employee after separation.
   iv. When deemed critical to ongoing business needs, access to the former employees email will be granted to departmental supervisors. Approval is required from either Human Resources or Legal Affairs.
   v. The use of an automated response/bounce message for former employees can be applied for 60 days from last day worked if approved by both the former employee's Supervisor and Human Resources. The messages must contain information for senders to direct questions for University business to a contact at Duquesne University and may contain new personal/business contact information for the former employee if appropriate and approved.

b. Student
   i. For graduated students, email is disabled 13 months after graduation. Email is purged 60 days following the end of the 13th month.
   ii. For students who leave before graduation, email is retained for 13 months from the last term they were registered. Email is purged 60 days following the end of the 13th month.
   iii. If a student graduates and then becomes an employee of the university and then separates from the university within the 13-month retention period, the email account is treated as an employee account and is handled as such (see section a. above).

c. Retiree
   i. As outlined in TAP 18, individuals who are defined as a “retiree” of the University are entitled to a Duquesne University email address.
   ii. Duquesne University retiree email accounts are offered for retirees. Retirees are required to follow all University policies, service requirements, and processes to retain the email account.
   iii. Email access will be disabled if the retiree has not accessed the account within the past 12 months.

d. Role Changes for Employees with Access to Restricted Data
   i. The University may require employees to be issued a new MultiPass account and email mailbox when the employee changes roles from one that has access
to Restricted Data to one that no longer is authorized to access that data. Examples may include: a Staff Member in HR who is no longer employed by the University but is still retains a student status or a Staff Member in CTS who no longer works for CTS but retains adjunct faculty status.

ii. When new MultiPass accounts and email mailboxes are issued, the employee is no longer permitted access to their prior email. This step is necessary to protect the potential sensitive data due to compliance and statutes.

e. Privacy and Right of University Access

While the University will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy of email sent through University Email Accounts (including email forwarded from University Email Systems).

Certain circumstances may require University members to access individual’s email accounts. These circumstances can include, but are not limited to: maintaining the system, investigating security or abuse incidents, business continuity, leaves, or separation from the University. Access to individual email accounts will be provided if approved by either Legal Affairs or Human Resources based on the University’s business needs.

7. Enforcement:

The unauthorized or improper use of Duquesne University’s technology environment, including the failure to comply with these service requirements, constitutes a violation which may result in the loss of access, University disciplinary actions and/or legal prosecution under federal, state and local laws, where applicable. Users are expected to adhere to T.A.P. 26 - Computing and Ethics Guidelines which can be found at http://www.duq.edu/taps.

The University reserves the right to amend these service requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws.

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Reason for Change</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/1/2018</td>
<td>Updates to policy</td>
<td>Tom Dugas, Chief Information Security Officer (CISO)</td>
</tr>
</tbody>
</table>