EMAIL POLICY

Policy Number: IT-7

Effective Date: July 1, 2002

Revision Date: July 1, 2014

Applicability: This policy applies to all persons using electronic mail services operated by or on behalf of Drexel University and its affiliates.

Responsible Officer: Vice President of Information Resources and Technology; Chief Information Officer, College of Medicine.

I. Purpose
Define appropriate use of email for transmitting electronic messages containing Drexel University information.

II. Definitions
Email Users: All Drexel University faculty, professional staff, students, consultants, and authorized others who are provided with email services by the University or its affiliates.

Sensitive Data: Protected Health Information, Social Security Numbers, Credit Card Numbers, Financial Account Numbers, and other information protected by HIPAA, FERPA, Gramm Leach Bliley, Pennsylvania Breach of Personal Information Notification Act and other laws and regulations.

Protected Health Information: Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

III. Policy
A. Use of University Email Accounts
Use of email services must comply with this, the Acceptable Use Policy IT-1, and other applicable University policies.

B. Encryption of Emails Containing Sensitive Data
Emails containing sensitive data must be encrypted by approved University email encryption software before being sent over a network. All emails containing sensitive information must be limited to minimum necessary information.

C. Prohibited Forwarding of Email
Automatic forwarding of mail to an outside third party mail system is prohibited for any correspondence that contains Sensitive Data.

Abuse of Email Privileges
Use of email is a privilege, not a right. This privilege can be revoked. Unacceptable behavior includes, but is not limited to:

1. Sending unsolicited and unauthorized mass email (spam)
2. Use of offensive language
3. Distribution of obscene material

4. Threats
5. Infringement on others' privacy
6. Interference with others' work
7. Copyright infringement
8. Illegal activity

Penalties for unacceptable behavior range from de-activation of the account (for minor first offenses) through university judicial action or referral to law enforcement authorities.

In the case of account de-activation, the offender’s account will only be reactivated upon the direction of the Chief Compliance and Privacy Officer.

Monitoring
Per the Acceptable Use Policy email communications may be audited to ensure compliance with set policies.

IV. Cross-Reference

1. Acceptable Use Policy (/irt/about/policies/policies/01-Acceptable-Use/) (IT-1)