# TITLE: ACCEPTABLE USE POLICY

**POLICY NUMBER:** IT-01
**EFFECTIVE DATE:** July 1, 2014
**REVISION DATE:** N/A
**SUPERSEDES**: NA
**RESPONSIBLE EXECUTIVE:** Vice President of Information Technology and Chief Information Officer

## I. PURPOSE AND APPLICATION

Drexel University's Acceptable Use Policy (AUP) sets forth the standards by which all students, faculty, staff and authorized guests (hereafter referred to collectively as "User(s)") may use their assigned computer accounts, email services and the shared Drexel University network. The use of Drexel's computer and network resources including all electronic communication systems and equipment (hereafter referred to collectively as the "Drexel Network") is a revocable privilege.

## II. SCOPE

This policy applies to the entire University community, faculty, professional staff, students, authorized guests, or a combination of these groups.

## III. IMPLEMENTATION

Implementation of this policy is the responsibility of the Chief Information Officer, Information Technology department. For inquiries regarding this Policy, please contact the Information Technology department at helpdesk@drexel.edu.

## IV. STATEMENT OF POLICY AND PROCEDURE

The Drexel network is provided to support Drexel University business and its mission of education, service and research. Any other uses, including uses that jeopardize the integrity of the Drexel Network, the privacy or safety of other Users, or that are otherwise illegal are prohibited.

By using or accessing the Drexel Network, Users agree to comply with the AUP and other applicable Drexel policies which may be implemented from time to time, as well as all Federal, state, local laws and regulations. Using and/or accessing the Drexel Network without proper authorization is strictly prohibited. Users should not have any expectation of privacy with regard to communications passed through the network or stored on computers that use it.

### A. Principles

General guidelines for acceptable use of the Drexel Network are based on the following principles:

1) Users must behave responsibly with respect to the Drexel Network at all times.

2) Users must respect the integrity and the security of the Drexel Network.

3) Users must behave in a manner consistent with Drexel's mission and comply with all applicable laws, regulations, and Drexel policies.

4) Users must be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use the Drexel Network and show restraint in the consumption of shared resources.

5) Users must respect the rights and property of others, including privacy, confidentiality and intellectual property.

### B. Access Requirements

The following statements govern access to the Drexel Network:

1) All access is denied unless expressly granted. Drexel University Information Technology generally grants access in the form of computer and network accounts to registered students, faculty, staff, and others as appropriate for such purposes as research, education (including self-study), or University administration. Passwords and/or personal identification numbers protect university accounts.

2) Accounts are assigned to individuals and are not to be shared unless specifically authorized by IT. Each User is solely responsible for all functions performed from accounts assigned to them. It is a violation of the AUP for any User to allow others (including other Users within the Drexel Network) to use or have access to their account. It is a violation to use another User's account, with or without that person's permission. Intentionally or negligently revealing one's password is prohibited. It is a violation to attempt to learn the password to another User's account, whether the attempt is successful or not

3) The password used with an account, is the equivalent of an electronic signature. The use of User ID and password authenticates an identity and gives on-line affirmations the force of a legal document.

4) Users are responsible for ensuring that they also comply with all IT policies, including those related to keeping the Drexel Network secure such as the Security of Information and Networked Systems Plan and the Security of Enterprise Systems Plan.

### C. Prohibitions

The following activities are specifically prohibited:

1) Users may not attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may not appropriate Drexel University's name, network names, network number spaces, or Drexel University logos, trademarks or servicemarks. Users may not use Drexel University's assigned Internet number space for their own domain without the prior express permission of IT.

**2)** Users may not attempt to intercept, monitor, forge, alter or destroy other Users' communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of the owner.

**3)** Users may not engage in actions that disrupt or interfere with the legitimate use by other Users of any computers and/or networks, including the Drexel Network, that interfere with the supervisory or accounting functions of the systems, or that are likely to have such effects. Such conduct includes, but is not limited to: placing of unlawful information on the system, transmitting data or programs likely to result in the loss of an individual's work or system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others, i.e. spam.

**4)** Users may not possess, distribute or send unlawful communications of any kind, including but not limited to threats of violence, obscenity, child pornography and/or harassing communications (as defined by law), or participate or facilitate communications in furtherance of other illegal activities.

**5)** Users may not attempt to bypass computer or network security mechanisms, including the Drexel Network, without the prior express permission of the owner of that computer or network system. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt. The unauthorized scanning of the Drexel Network is also prohibited.

**6)** Users must obey all established guidelines for any computers or networks used, both inside and outside Drexel University. For example, individuals using computing resources provided by IT, Drexel University Libraries, individual Colleges, Schools or Departments must adhere to the policies established for use of those resources. Users accessing off-campus computers via external networks must abide by the policies established by the off-campus owners of those computers and networks as well.

**7)** Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permissions of the copyright holder. Information on the Digital Millennium Copyright Act can be found at: http://www.copyright.gov/legislation/dmca.pdf (PDF file) and the Copyright Act at: http://www.copyright.gov/title17/

**8)** Users may not use the Drexel Network for private business, commercial or political activities, fundraising, or advertising on behalf of non-Drexel organizations, unlawful activities or uses that violate other Drexel University policies. Users may not extend or share the Drexel Network.

**9)** Users may not violate any laws or ordinances, including, but not limited to, copyright, discrimination, harassment, and/or export controls. Drexel University may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

The use of the Drexel Network is also required to conform to the following Drexel University policies:

1) CPO-1 The Code of Conduct
2) OED-1 Equality and Non-Discrimination Policy
3) OED-2 Reasonable Accommodation of Individuals with Disabilities
4) OED-3 Sexual Harassment and Misconduct Policy

### D. Monitoring

Drexel University reserves the right to review and/or monitor any emails or transmissions sent or received through the Drexel Network, at its sole discretion.

Penalties for violating the AUP may include restricted access or loss of access to the Drexel Network, termination and/or expulsion from Drexel University and in some cases, civil and/or criminal liability.

Drexel University reserves the right to update or revise the AUP or implement additional policies in the future. Users are responsible for staying informed about Drexel University policies regarding the use of computer and network resources and complying with all applicable policies.

## V. KEYWORDS AND DEFINITIONS

N/A

## VI. RELATED POLICIES, FORMS AND RESOURCES

### A. Related Policies

CPO-1 The Code of Conduct
OED-1 Equality and Non-Discrimination Policy
OED-2 Reasonable Accommodation of Individuals
OED-3 Sexual Harassment and Misconduct Policy

### B. Forms and Resources

N/A

## VII. POLICY HISTORY

Revision Date: July 1, 2014