Purpose:
This policy provides notice of the expectations and guidelines of Fordham University (the University) to all who use and manage Information Technology (IT) resources and services. The University provides IT Resources for the advancement of the University’s educational, research, service, and business objectives. Any access or use of IT Resources that interferes, interrupts, or conflicts with these purposes is not acceptable and will be considered a violation of this policy.

Scope:
This policy, and all policies referenced herein, apply to all members of the University community including faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the “User(s)” or “you”) who use, access, or otherwise employ, locally or remotely, the University’s IT Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions:
IT Resources include, computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
Table of Contents:
1. User Responsibilities and Statement of Prohibited Uses ......................................................... 3
   A. Spirit of Use .......................................................................................................................... 3
   B. User Names ......................................................................................................................... 3
   C. Passwords ............................................................................................................................ 3
   D. Additional Responsibilities ................................................................................................. 4
   E. Additional Prohibited Uses ................................................................................................. 5
2. Intellectual Property ................................................................................................................ 6
3. Privacy ...................................................................................................................................... 7
4. Monitoring, Reporting, Violations, and Sanctions ................................................................. 8
   A. Monitoring ........................................................................................................................... 8
   B. Reporting ............................................................................................................................ 8
   C. Violations ............................................................................................................................. 9
   D. Sanctions ............................................................................................................................. 9
5. User Obligation to Review ....................................................................................................... 9
Policy Statement:

1. User Responsibilities and Statement of Prohibited Uses

A. Spirit of Use

Only authorized Users have the privilege to access and use the IT Resources. Access and use is limited to the purposes that are consistent with the instructional, research, and administrative goals of the University.

Users are expected to uphold the standards and principles of the University while using the IT Resources and are required to respect the rights of others at all times. Users are prohibited from using any portion of the IT Resources to post or transmit any information, including data, text, files, links, software, chat, collaboration, communication, or other content (Content) that is abusive, disparaging, discriminatory, hostile, combative, threatening, harassing, intimidating, defamatory, pornographic, or obscene. Users who do not respect the Spirit of Use of IT Resources may be held in violation of this policy.

B. User Names

The University recognizes that common practice in computing, online or otherwise, involves use of a “user name”, “login”, “AccessIT ID”, or “screen name” (collectively, “user name”) that may be different from the User’s legal name. Using someone else’s name or assuming someone else’s identity without appropriate authorization, however, is a violation of the University’s principles and this policy.

Users may not use the IT Resources under false name, identification, email address, signature, or other medium of any person or entity without proper authorization. The University prohibits such use of a User name for the purposes of misrepresentation or an attempt to avoid legal or other obligations. Any such unethical use may constitute a violation of this policy.

C. Passwords

When choosing a password for access to the IT Resources, or portions thereof, Users are must adhere to the following rules so as to prevent unauthorized access through any User’s password.

1. Use a different password for each account; and
2. Do not write down your password(s) on a piece of paper or record them in a file.
3. Users should avoid using:
IT Policy: Acceptable Uses of IT Infrastructure and Resources
Version 3.0

a. Birth dates;
b. Names (First, Last, or any combination);
c. Unaltered words that could be found in a dictionary, including non-English words, and words spelled backwards;
d. Telephone numbers;
e. Social Security numbers;
f. Fordham Identification Numbers (FIDN);
g. Famous or other proper names; and
h. Alphabet or keyboard sequences (e.g. “QWERTY”).

When using Fordham’s AccessIT ID, your password must meet the following criteria:

1. Your password must be 8 characters or more;
2. Your password must contain at least 1 numeric;
3. Your password must contain at least 1 uppercase and 1 lowercase character;
4. Your password must not be reused; and
5. Your password must not contain any of the following special characters: @&/;
6. You should change your password every 180 days.

Users should not have an expectation of privacy in content either located in the University’s IT Resources or the User’s own system, whether that content is protected by a user name and password, or otherwise.

D. Additional Responsibilities

All Users must fully comply with the standards and responsibilities of acceptable use as outlined in:

1. All applicable provisions of the University Code of Conduct, employee handbooks and agreements, student handbooks and other policies and procedures established by the undergraduate, graduate, and professional schools of the University;
2. This IT Policy in its entirety including the related policies as defined in the Related Policies and Procedures section;
3. All local, state, federal, and international laws;
4. All application and/or software license agreements acquired by the University and its authorized units;
5. All applicable University policies and procedures including sexual harassment, academic dishonesty, scientific misconduct, and non-discrimination; and

6. The legal and educational standards of software use as published in the EDUCOM Code.

Users must adhere to the following responsibilities:

1. Self-policing of passwords and access codes as set forth above;
2. Respecting authorial integrity and the intellectual property rights of others;
3. Respecting and protecting the confidentiality, integrity, and availability of all University IT Resources;
4. Ensuring that all data and files that the User accesses, transmits, and/or downloads are free from any computer code, file, or program which could damage, disrupt, expose to unauthorized access, or place excessive load on any computer system, network, or other IT Resource;
5. Reporting any security risk or code, file, or program, including computer viruses, Trojan Horses, worms, or any other malware that affects any IT Resource including any owned or operated by the User; and
6. Properly backing up appropriate User systems, software, and data.

E. Additional Prohibited Uses

Users are prohibited from accessing or using the IT Resources in the following manners:

1. Initiating or participating in unauthorized mass mailings to news groups, mailing lists, or individuals, including, but not limited to, chain letters, unsolicited commercial email (commonly known as “spam”), floods, and bombs;
2. Giving others, by password or other means, unauthorized access to any User account or the IT Resources;
3. Seeking to, without authorization, wrongly access, improperly use, interfere with, dismantle, disrupt, destroy, or prevent access to, any portion of the IT Resources including User or network accounts;
4. Violating or otherwise compromising the privacy, or any other personal or property right, of other Users or third parties through use of the IT Resources;
5. Disguising or attempting to disguise the identity of the account or other IT Resource being used including “spoofing” resource addresses, impersonating any
other person or entity, or misrepresenting affiliation with any other person or entity;

6. Using the IT Resources to gain or attempt to gain unauthorized access to networks and/or computer systems;

7. Engaging in conduct constituting wasteful use of IT Resources or which unfairly monopolizes them to the exclusion of others;

8. Engaging in conduct that results in interference or degradation of controls and security of the IT Resources;

9. Unless expressly authorized by the University in writing, exploiting or otherwise using the IT Resources for any commercial purpose;

10. Engaging in computer crimes or other prohibited acts;

11. Intentionally or unintentionally violating any applicable local, state, federal, or international law;

12. Knowingly or negligently running, installing, uploading, posting, emailing, or otherwise transmitting any computer code, file, or program, including, but not limited to, computer viruses, Trojan horses, worms, or any other malware, which damages, exposes to unauthorized access, disrupts, or places excessive load on any computer system, network, or other IT Resource; and

13. Using any IT Resource, including email or other communication system to intimidate, insult, embarrass, or harass others; to interfere unreasonably with an individual’s work, research, or educational performance; or to create a hostile or offensive environment.

Periodically, the University will conduct information sessions to present, or provide through official communications, specific examples of inappropriate uses of the IT Resources. In the interest of creating a well-informed User community, the University also encourages questions about proper use. Please direct inquiries to Fordham IT Customer Care at (718) 817-3999, or the Office of Legal Counsel at (718) 817-3110.

2. Intellectual Property

As each User should have an expectation that others will not abuse his or her intellectual property rights, every User must also respect the intellectual property rights of others including those of other Users, all members of the University community, and all third parties.

Potential violation of intellectual property laws and rights is not merely limited to unauthorized downloading of copyrighted movies, television shows, music, and software through file-sharing software. Rather, the concept of intellectual property broadly covers all copyrighted works, trademarks, patents, and other proprietary and confidential information.
The University requires every User to adhere to a strict policy of respecting intellectual property rights. Infringing and illegal uses may involve:

- Unauthorized copying or sharing of written works, such as textbooks and course materials;
- Unauthorized copying, sharing, and use of digital videos or images, digital music as well as logos and other marks;
- Unauthorized copying, sharing, or installation of software, including commercially licensed software as well as “shareware”;
- Unauthorized copying, sharing, or use of copyrighted, or otherwise proprietary, data or collections of data.

It is the responsibility of every User to avoid infringing any intellectual property right and to report the infringement of another User if and when it is discovered. Failure to respect such rights, or report infringements, is a violation of this policy and subject to the sanctions set forth below.

3. Privacy

The University reserves the right to access, inspect, examine, monitor, intercept, remove, restrict, and take possession of all University owned and operated IT Resources, including but not limited to, electronic mail network connectivity, hard disks, printed media, devices, data, software, printers, voice mail, removable media, fax machines, scanners, computers, mobile devices, telephony equipment, connected devices, laptops, documents, and other files.

The University also reserves the right to access, inspect, examine, monitor, intercept, remove and restrict use and access to the IT Resources indicated above.

The University may exercise these rights for various reasons, including but not limited to:

- Ascertaining whether Users are using the systems in accordance with the IT Policy and other university guidelines;
- Preventing, investigating, or detecting unauthorized use of the University’s systems;
- Ensuring compliance with applicable laws and regulations.

Users are expected and obligated to use such IT resources in a manner consistent with the purposes, objectives, and mission of the University and this policy.

Except where applicable law provides otherwise, Users should have no expectation of a reasonable level of privacy while accessing or using University’s IT Resources. For example, issuance of a password or other means of access is to assure appropriate confidentiality of University-related information and files. However, it does not guarantee privacy, especially for personal or unlawful use of IT Resources.
Users should note that the University may also require back-up and caching of various portions of the IT Resources; logging of activity; monitoring of general usage; and other activities that are not directed against any individual User or User account, for protecting the University’s IT Resources and systems, maintaining security and maintenance, or restoring normal operations of the IT Resources.

The University reserves the right to examine, use, and disclose any data or Content found on the University’s IT Resources for the purposes of furthering the health, safety, discipline, legal rights, security, or intellectual or other property of any User or other person or entity. Information that the University gathers from such permissible monitoring or examinations may also be used in disciplinary actions. Such information may be disclosed to law enforcement officials when necessary.

Users are responsible for the security of their own User IDs and passwords. Passwords must not be shared with other persons.

4. Monitoring, Reporting, Violations, and Sanctions

A. Monitoring

As noted above, the University may, but is not required to, monitor, block, or otherwise prevent inappropriate use of the IT Resources. Nonetheless, in the event of a violation or failure to comply with this policy, the University may monitor any User’s access and use of the IT Resources in order to determine whether violations are taking place. If violations are found, the University may initiate charges and impose appropriate sanctions by following the various processes and procedural safeguards that are applicable to the User’s employment or enrollment status.

B. Reporting

Users have an obligation to report violations of the IT Policy as well as any potential security or other breach of any portion of the IT Resources. Reporting of any such violations or other issues involving the inappropriate use of the IT Resources should be referred to:

- The Dean of Students (or delegate) if the alleged offender is any student on any campus except students in the School of Law;
- The Academic Dean (or delegate) in the School of Law, if the alleged offender is a student therein;
- The Area Vice President, if the alleged offender is an administrator;
- The appropriate Academic Dean or Provost, if the alleged offender is a faculty member;
IT Policy: Acceptable Uses of IT Infrastructure and Resources
Version 3.0

- The Vice President for Development and University Relations, if the alleged offender is an alumnus of the University;
- The Vice President of Human resources (or delegate), if the alleged offender is any other employee who does not fall into any of the above categories; or
- The Associate Vice President for Information Technology/CISO, for all other alleged offenders.

C. Violations

A violation of the IT Policy is considered a violation of the University’s principles, objectives, and standards. Depending on the severity of violation, it may also violate the University’s other policies or even local, state, federal, or international law. The University may impose penalties ranging from the termination of the User’s access to the IT Resources to disciplinary review and further action including non-reappointment, discharge, or dismissal. In cases involving egregious violations, the University may institute legal action or cooperate with an action brought by applicable authorities or third parties.

D. Sanctions

Users who fail to fulfill their responsibilities and engage in prohibited conduct are subject to sanctions imposed by the University. Sanctions against students are listed in the Student and Residential Life Handbooks. Faculty are subject to disciplinary action including reprimand, suspension, and dismissal as stipulated in Article IV of the University Statutes. Administrators and staff are subject to disciplinary action under their respective handbook and collective bargaining agreements. Depending on the nature and severity of the violation, sanctions can range from various levels of warnings to immediate termination of employment or enrollment.

The University will exercise good faith and proper discernment in its enforcement of the IT Policy. It will respect the academic freedom to which Users are entitled insofar as the legal rights and responsibilities of the individual User and the University require. Under no circumstance shall the University be liable to any User or third party for any violation including illegal or improper acts that any User commits through use of the IT Resources.

5. User Obligation to Review

The University will periodically update this policy. By accessing and using the IT Resources, each User represents and acknowledges that he or she has checked and read this policy on a regular basis so as to be informed of any changes hereto. If any User does not agree to check the IT Policy for revisions on a regular basis, said User may not use the IT Resources. Changes to the policy are noted in the Revision History table found later in this document.
IT Policy: Acceptable Uses of IT Infrastructure and Resources

Version 3.0

Related Policies and Procedures:
The term IT Policy shall also include any additional University policies related to Information Technologies, either issued by the Office of Legal Counsel or Fordham IT. Additional Fordham IT issued policies can be found on the Fordham IT web pages.

The University may at times contract with software application vendors or providers of other IT services. Such third-party providers may post their own policies that apply to Users. You must comply with such policies when using third party software, applications, or other IT services through the University’s IT Resources.

Implementation Information:

<table>
<thead>
<tr>
<th>Review Frequency:</th>
<th>Annual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Person:</td>
<td>Director, IT Risk and Data Integrity</td>
</tr>
<tr>
<td>Approved By:</td>
<td>CISO and Office of Legal Counsel</td>
</tr>
<tr>
<td>Approval Date:</td>
<td>December 20, 2017</td>
</tr>
</tbody>
</table>

Revision History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>12/04/2004</td>
<td>Initial Acceptable Use Policy, which includes Applicability, User Responsibilities, and Statement of Prohibited Uses, Enforcement, and Sanctions for Non-Compliance, Privacy, and Emergencies Sections. Additionally, added as addendums policies for Anti-Spam, Email, Peer-to-Peer, Web Hosting, and Wireless Policies.</td>
</tr>
</tbody>
</table>
The policy was extensively reviewed and modified by the Office of Legal Counsel. The following changes were made:

1. General addition of terms, modification of language, and reorganization of sections and sub-sections to the entire IT Policy;
2. Addition of “User Names” and “Passwords” sub-sections to “User Responsibilities and Statement of Prohibited Uses” section;
3. Addition of “Intellectual Property” section;
4. Addition of sub-sections and reorganization of former “Enforcement and Sanctions for Non-Compliance” and “Emergencies” sections, now, collectively, the “Monitoring, Reporting, Violations, and Sanctions” section;
5. Addition of the “Amendments and Revisions” section in its prior format; and
6. Addition of the “Internet Usage Policy” as an addendum.

This revision includes:

1. Changes in the password section because of the deployment of AccessIT ID,
2. A change in Section 5, sub-section B, “Reporting,” which moved the reporting of an incident that involves a student in the Graduate School of Arts and Sciences to the Academic Dean of the school instead of the Dean of Students,
3. Grammatical corrections throughout multiple sections of this document.

This revision includes:

1. Modifications to the Peer to Peer Policy to meet the requirements of the Higher Education Opportunity Act of 2008.

This revision includes:

1. Addition of the password change policy of 180 days.
IT Policy: Acceptable Uses of IT Infrastructure and Resources

Version 3.0

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4</td>
<td>08/19/2016</td>
<td>This revision includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Addition of Section XIII Core Google Apps Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Addition of Section XIV Non-core Google Apps Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Minor grammatical changes</td>
</tr>
<tr>
<td>2.5</td>
<td>12/14/2016</td>
<td>This revision includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Modifications to the Peer-to-Peer Policy that reflect new restrictions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>on peer-to-peer file sharing that are effective as of January 4, 2017.</td>
</tr>
</tbody>
</table>
The policy has been renamed from IT Acceptable Use to Acceptable Uses of IT Infrastructure and Resources. In a joint effort between the Office of Legal Counsel and Fordham IT, major revisions have occurred. These revisions include:

- The reformatting of the policy into the Fordham IT template for policies so that all policies are consistent.
- The removal of sections from this policy. These sections will now be contained in their own standalone policies. The sections removed are as follows:
  - Anti-Spam
  - Email
  - Peer-to-Peer
  - Hosting
  - Wireless
  - Internet Usage
  - Core Google Services
  - Non-Core Google Services
- Placement of the IT Policy Statement, Applicability, and Related Policies sections of the old policies into the appropriate areas of the IT Policy Template.
- Elimination of the Current Revision section as that is incorporated in this table.
- Streamlining of the Password section
- Modernization of the Intellectual Property section
- Rewrite of the Privacy section to reflect changes in privacy regulations that the University is required to adhere to.
- Updates to the Reporting section.