# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>IT Policy Statement</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>A. Applicability</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>B. Related Policies</td>
<td>3</td>
</tr>
<tr>
<td>II.</td>
<td>User Responsibilities and Statement of Prohibited Uses</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>A. Spirit of Use</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>B. User Names</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>C. Passwords</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>D. Additional Responsibilities</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>E. Additional Prohibited Uses</td>
<td>6</td>
</tr>
<tr>
<td>III.</td>
<td>Intellectual Property</td>
<td>7</td>
</tr>
<tr>
<td>IV.</td>
<td>Privacy</td>
<td>8</td>
</tr>
<tr>
<td>V.</td>
<td>Monitoring, Reporting, Violations, and Sanctions</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>A. Monitoring</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>B. Reporting</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>C. Violations</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>D. Sanctions</td>
<td>9</td>
</tr>
<tr>
<td>VI.</td>
<td>Amendments and Revisions</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>A. User Obligation to Review</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>B. Current Revision</td>
<td>10</td>
</tr>
<tr>
<td>VII.</td>
<td>ANTI-SPAM POLICY</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>A. Email Anti-Relay Policy</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>B. Bulk Email Policy</td>
<td>11</td>
</tr>
<tr>
<td>VIII.</td>
<td>EMAIL POLICY</td>
<td>12</td>
</tr>
<tr>
<td>IX.</td>
<td>PEER-TO-PEER POLICY</td>
<td>13</td>
</tr>
<tr>
<td>X.</td>
<td>HOSTING POLICY</td>
<td>15</td>
</tr>
<tr>
<td>XI.</td>
<td>WIRELESS POLICY</td>
<td>16</td>
</tr>
<tr>
<td>XII.</td>
<td>INTERNET USAGE POLICY</td>
<td>17</td>
</tr>
<tr>
<td>XIII.</td>
<td>CORE GOOGLE SERVICES POLICY</td>
<td>18</td>
</tr>
<tr>
<td>XIV.</td>
<td>NON-CORE GOOGLE SERVICES POLICY</td>
<td>19</td>
</tr>
</tbody>
</table>
FORDHAM UNIVERSITY

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. IT Policy Statement

This Policy Statement provides notice of Fordham University (hereinafter the “University”)’s expectations and guidelines to all who use and manage information technology (hereinafter “IT”) resources and services (including but not limited to computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, and any related materials and services) (hereinafter the “IT Resources”).

The University provides the 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 Statement (hereinafter the “IT Policy”).

A. Applicability

This IT Policy, and any other policy referenced herein, shall apply to any and every member of the University community including, but not limited to, faculty, students, administrative officials, staff, and independent contractors (hereinafter the “User(s)” or “you”) who uses, accesses, or otherwise employs, locally or remotely, the University’s IT Resources, whether individually controlled, shared, stand-alone, or networked.

B. Related Policies

The term IT Policy shall also include any additional University policies related to information technologies, all of which are incorporated herein by reference. Such topically oriented policies include, but are not limited to, the Anti-Spam Policy, the Email Policy, the Peer-to-Peer Policy, the Web Hosting Policy, the Wireless Policy, and the Internet Usage Policy, all of which are set forth below.

Further, all such Users accessing and using IT Resources are subject to this IT Policy in addition to applicable provisions of the University Statutes, the University Code of Conduct, the Handbook for Administrators, Local 153 and Local 805 Collective Bargaining Agreements, Student Handbooks, and all other policies and procedures established by the schools and administrative offices of the University.

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

II. User Responsibilities and Statement of Prohibited Uses

A. Spirit of Use

Only authorized members of the University community are extended 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 and the User’s relationship to those goals.
Moreover, as members of the University community, Users are expected to uphold the standards and principles of the University while using the IT Resources. Accordingly, Users 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, data, text, file, link, software, chat, communication or other content (hereinafter, collectively, “Content”) that is harmful, abusive, discriminatory, hostile, combative, threatening, insulting, embarrassing, harassing, intimidating, defamatory, pornographic, obscene, or which negatively affects the University, another User, or any third party. Users who do not respect the Spirit of Use of the IT Resources may be held in violation of this IT 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 IT Policy.

Accordingly, 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. Thus, 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 IT Policy.

C. Passwords

When choosing a password for access to the IT Resources, or portions thereof, Users are expected to follow the University’s “best practices” so as to prevent unauthorized access through any User’s password. Accordingly, Users should avoid using:

1. Birth dates;
2. Names (First, Last, or any combination);
3. Unaltered words that could be found in a dictionary, including non-English words and words spelled backwards;
4. Telephone numbers;
5. Social security numbers;
6. Fordham Identification Numbers (FIDN)
7. Famous or other proper names; and
8. 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 between 8 and 32 characters;
2. Your password must contain 1 numeric;
3. Your password must contain at least 1 uppercase and 1 lowercase character;
4. Your password must not be the same as your last 5 passwords; and
5. Your password must not contain any of the following special characters:
~!@#$%^&*() _+=-`{}|\:";'",<>?/

6. You must change your password at most every 180 days.

Other best practices that Users should follow include:

1. Using a different password for each account; and
2. Not writing down your password(s) on a piece of paper or recording them in a file on any computer.

Users should always bear in mind that, even when employing best practices, breaches can occur in any number of points in both the IT Resources or the User’s own system(s). Accordingly, in addition to the provisions regarding privacy set forth below, Users should not have an expectation of privacy in any 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

In consideration of the privilege of accessing and using the IT Resources, 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: Anti-Spam Policy, Email Policy, Peer-to-Peer Policy, Hosting Policy, Wireless Policy, and Internet Usage Policy;
3. All local, state, federal, and international laws;
4. All software license agreements acquired by the University and its authorized units;
5. All applicable University policies and procedures including, but not limited to, 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.

Moreover, Users must adhere to the following responsibilities:

1. Self-policing of passwords and access codes per the best practices set forth above;
2. Respecting authorial integrity and the intellectual property rights of others;
3. Respecting and protecting the integrity, availability, and security of all University IT Resources;
4. Ensuring that all data and files that the User accesses 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, but not limited to, computer viruses, Trojan Horses, worms, or any other “mal-ware”—that infects 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

In addition to other prohibitions found in this IT Policy and any other applicable University code, statute, handbook, policy, or procedure, Users are prohibited from accessing or using the IT Resources in the following manners or for the following purposes:

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, in whole or part;

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, but not limited to, “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 remote networks, including remote 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 “mal-ware”—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 e-mail 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 working or learning 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 at (718) 817-3999, or the Office of Legal Counsel at (718) 817-3111.

III. Intellectual Property

The University takes the issue of intellectual property and similar rights seriously. Many members of the University community hold patents. Virtually all members of the faculty and student body have copyrights merely by authoring a paper whether for publication or even through a course assignment. Accordingly, 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 music through file-sharing software. Rather, the concept of intellectual property broadly covers all copyrighted works, trademarks, patents, trade dress, trade secrets, and other proprietary and confidential information. Thus, intellectual property issues likely apply to any and all Content that a particular User did not generate him or herself and to which a User has not been given rights.

Accordingly, the University requires every User to adhere to a strict policy of respecting intellectual property rights. Infringement of recorded music, in various forms including but not limited to MP3 files, is a matter of concern to the University. Other potentially infringing uses may involve:

- Unauthorized copying of written works, including but not limited to textbooks and course materials;
- Unauthorized copying and use of digital videos or images, as well as logos and other marks;
- Unauthorized copying or installation of games or other software, including “shareware”; and
- Unauthorized copying or use of copyrighted, or otherwise proprietary, data or collections of data.
These are just a few examples of potential infringement that Users may intentionally or unintentionally commit.

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 IT Policy and subject to the sanctions set forth below.

IV. Privacy

All Users retain the right of privacy in their personal files and data, electronic mail, and voice-mail as long as they are using the IT Resources in a manner consistent with the purposes, objectives, and mission of the University and this IT Policy. Likewise, Users are obligated to respect the right of privacy that other Users have in their own systems, data, and accounts.

Users should be aware that the University cannot guarantee security and privacy during use of the IT Resources. To the contrary, various uses of the IT Resources, or access in general, may not always be private. 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 in all cases, especially for personal or unlawful use of IT Resources.

Moreover, Users should note that the University, in emergency situations, 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 the purposes of emergency maintenance or restoring normal operations of the IT Resources.

In the event the University has reasonable suspicion that a User has violated any civil or criminal law, the University Code of Conduct, the IT Policy, or any other University policy, procedure, or regulation, the University reserves the right to access, inspect, monitor, remove, take possession of, or surrender to civil or criminal authorities the offending Content, with or without notice or consent of the User. The University may also do so for the purpose of satisfying any law, regulation, or government request.

Further, the University may monitor the IT Resources to ensure that they are secure and being used in conformity with this IT Policy and other University guidelines. Thus, to the extent allowed by applicable law, 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, 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.

This limited exception to the general right of privacy in the context of acceptable use of IT Resources can be authorized for reasonable cause only by a duly elected officer of the University—namely, the President and Vice Presidents and, in the case of faculty, with notice to the President of the Faculty Senate. Any action taken by the University based on the Content or information obtained will be subject to the procedural safeguards accorded under the University Statutes, Handbook for Administrators, Local 153 and Local 805 Collective Bargaining Agreements, the Student Handbooks, and all other student policies and procedures promulgated by the Student Affairs Division and the graduate and professional schools of the University.
V. 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 IT 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 an undergraduate student or a student in the Graduate School of Education, or Graduate School of Religion and Religious Education;
- The Academic Dean (or delegate) in the School of Law, Graduate School of Business, Graduate School of Arts and Sciences, and Graduate School of Social Service, if the alleged offender is a student therein;
- The Area Vice President, if the alleged offender is an administrator;
- The appropriate Academic Dean or Vice President for Academic Affairs, if the alleged offender is a faculty member;
- The Executive Director of Human Resources, if the alleged offender is any other employee who does not fall into any of the above categories; or
- The Vice President for Information Technology/CIO, 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. Accordingly, in response to any given violation, 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, but not limited to, 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

In addition to liability and penalties that may be imposed on a User under international, federal, state, or local laws, 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. Failure to take action in any particular instance does not constitute an alteration of the IT Policy or a waiver of any right or remedy available to the University. Under no circumstance shall the University be liable to any User or third party for any violation including, but not limited to, illegal or improper acts, that any User commits through use of the IT Resources.

VI. **Amendments and Revisions**

A. **User Obligation to Review**

Just as technology is constantly evolving, so are the policies that address it. Accordingly, the University will periodically update this IT Policy. By accessing and using the IT Resources, each User represents and acknowledges that he or she has checked and read this IT 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.

B. **Current Revision**

The current version of this IT Policy was first posted on December 14, 2016. This policy supersedes the policy of August 19, 2016. The most recent revision includes:

1. Modifications to the Peer-to-Peer Policy that reflect new restrictions on peer-to-peer file sharing that are effective as of January 4, 2017.
VII. ANTI-SPAM POLICY

Unsolicited commercial email, commonly referred to as “Spam”, includes, but is not limited to, advertising email, email containing pyramid schemes, chain letters, emails containing unwanted questionable subject matter, and abusive or threatening email. Spam is often denoted by email that contains a false or misleading header, subject-line, identification of the sender, return address, routing or transmission path, or other false indication of origin, sometimes using a third party domain name without permission. In addition, Spam includes email that advertises goods or services that has been sent without the consent of the recipient, or without a preexisting relationship between the sender and recipient.

The University’s goal is to minimize the impact of Spam on the User community and IT Resources by implementing appropriate policies and technology. Users and third parties are prohibited from using the University’s IT Resources to send Spam or to send any electronic correspondence in violation of this IT Policy or any applicable policy, law, rule, or regulation pertaining to unsolicited or bulk messages. The University reserves the right to refuse email or other connections from outside hosts that send any messages that appear to be unsolicited, meant for mass distribution, commercial in nature without prior approval of the intended User-recipient, prurient, offensive, or containing viruses, worms, or other malicious computer code. The University will use all available technology at its disposal to block such Spam.

To make certain that email is a resource readily available, Users should note the following:

A. Email Anti-Relay Policy

Email relay is the transparent transmission of email between networked systems either local or on the Internet. The problem with email relaying is that, if not configured properly within an institution, it can be misused. For example, it might be used by anyone in the world to send bulk mailings while masking or concealing the identity of the sender. To curtail abuse, only those individuals who are identifiable Users of the University community may access and use the IT Resources’ email sending capabilities.

B. Bulk Email Policy

Bulk emailing, or email “bombing”, is characterized by abusers repeatedly sending an email message to a particular address or addresses at a specific victim site or address. In many instances, the messages are large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be compromised, increasing what is called a “denial of service” impact. The University will not tolerate the targeting of a User’s email account, or any combination of User accounts, by another User or third party, where such targeting appears to be for the purposes of harassing, irritating, or interfering with that User’s or those Users’ normal use of email. Accordingly, Users are prohibited from using the University’s systems to damage, disable, overburden, or impair any of the IT Resources, or analogous third-party systems and resources. Such violations will be referred to the appropriate University or outside authorities in accordance with this IT Policy.
VIII. EMAIL POLICY

Any User’s use of the University’s email system, like all of the IT Resources, is to be used only in support of our educational, research, and administrative mission and must be in conformity with the general IT Policy and compliant with all applicable law. Accordingly, Users must use this resource in an efficient, effective, ethical, and lawful manner. Email communications should reflect, rather than undermine, the University’s reputation and standard of excellence. Violation of the Email Policy may result in sanctions.

In addition to the User’s obligation to adhere to the Anti-Spam Policy above, Users are prohibited from sending mass or bulk emails or messages to other Users if such emails or messages do not further the University’s goals, interests, or educational mission. For the purposes of this policy, “mass” or “bulk” emails or messages include, but are not limited to, any such email or message that is sent to:

- More than 50 recipients;
- Any number of undisclosed recipients;
- One or more pre-defined group of email addresses or list addresses which distribute(s) the email or message to all Users within the group(s); and
- Any number of recipients if the identity of the sender is undisclosed or masked.

All network and email accounts maintained on and through the IT Resources are the sole property of the University. The University has the right, but not the obligation, to monitor any email account for legitimate business reasons. Reasons for review include, but are not limited to:

- Reasonable suspicion of a violation of the IT Policy or any other rule, law, or property right of another User or third party;
- Investigation of system problems;
- Litigation or anticipated litigation; or
- Any other technical or legal obligation or responsibility.

To the greatest extent possible, the University will attempt to preserve the privacy of any User whose email account is accessed or monitored. However, Users of the University’s email system must understand that all communications created, received, archived, or backed-up through the IT Resources may be subject to requests for public disclosure. Accordingly, Users should have no absolute expectation of privacy or confidentiality for data, documents, messages, and other materials stored or transmitted on or through the IT Resources, including via email accounts.
IX. PEER-TO-PEER POLICY

Peer-to-peer applications are defined as programs which allow computers to share data in the form of music, movies, games, or any computer file or software over a local network and the Internet without accessing a centralized distribution server or set of servers. The University prohibits and blocks the use of peer-to-peer applications on networks within the residence halls and public WiFi (Fordhamwifi) networks as of January 4, 2017 as directed by the University’s Information Risk Management Board. Usage of peer-to-peer applications is not restricted on any other network or Fordham IT resource at this time. Regardless, the use of these applications has been known to cause problems which can affect the entire University community as well as individual Users.

The University mandates that all IT Resources be used in a manner consistent with the IT Policy and compliant with The Higher Education Opportunity Act and all other applicable laws and regulations. The University is under no obligation to protect a User from a complaint or action arising from any violation, or alleged violation, of the law, including infringement of any intellectual property right due to use of peer-to-peer, or any other type of “file-sharing,” software or networks. Users should understand that the fact that material is accessible through the Internet does not mean that accessing such material is authorized by third party rights-holders. In some cases, even Content that is only accessible after a User pays for it may not be authorized for distribution by those who hold rights to that Content.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the U.S. Copyright Office website at www.copyright.gov, specifically FAQ's at www.copyright.gov/help/faq.

Accordingly, the University prohibits the use of peer-to-peer applications on its networks, including those networks where peer-to-peer file sharing is allowed, or the IT Resources, in general, to transmit or exchange any videos, music, software, images, or other Content, in which the intellectual property is held by any party or entity other than the User, unless the User has valid, written authorization to access or distribute such Content. Any use of the IT Resources in violation of this policy will be subject to disciplinary sanctions in keeping with the applicable provisions of the IT Policy and other University statutes, rules, and policies. Nonetheless, the University allows and encourages the use of peer-to-peer applications for legitimate academic purposes when such uses do not involve any violation of applicable laws, statutes, or policies, or infringement of third party rights.
The University will continue to implement safeguards against the illegal exchange and distribution of copyrighted materials. To that end, the University employs various deterrents such as bandwidth management technology to ensure peer-to-peer programs do not degrade network speeds or any other portion of the IT Resources. Currently, FordhamIT uses Packeteer to perform this work but reserves the right to install or change packet shaping and traffic monitoring technologies at any time. Nonetheless, should such programs degrade the performance of the IT Resources, or otherwise affect them in a manner inconsistent with the IT Policy or other University policies, appropriate action will be taken against the User or Users responsible for such degradation or other negative impact.

The University understands that there are legitimate academic uses for peer-to-peer applications. If you believe you have an academic justification for the use of P2P in the residence halls or public WiFi (Fordhamwifi), a request for an exception may be submitted to IT Customer Care. Go to the Tech Help tab at My.Fordham.edu and submit a self-service request by selecting the following categories: IT Services> Security> IT Security> Peer-to-Peer Exclusion Request. Exception requests will be reviewed on a case-by-case basis with department chairs, deans and vice presidents. If such exception is granted, it is expected that the User will strictly abide by the usage of the peer-to-peer file sharing policy by not sharing material that will infringe a copyright on another’s intellectual property. As such, Fordham University reserves the right to revoke peer-to-peer access granted by the exception process at any time if the User is suspected of sharing material that infringes a copyright or violates usage of intellectual property.

Users should be aware that peer-to-peer applications are not necessarily harmless and using them, in addition to potentially degrading the IT Resources’ performance, may:

- Violate copyright, patent, trademark, or other rights;
- May result in the disclosure confidential information; and
- May jeopardize the security of the IT Resources.

As noted above, disproportionate bandwidth usage and the unauthorized use or distribution of copyrighted materials constitutes a violation of the University’s IT Policy. The IT department of the University will annually review its peer-to-peer policy and procedures to ensure the utmost compliance with all applicable laws and regulations. To see a list of alternatives for legal downloading, please visit [http://www.educause.edu/legalcontent](http://www.educause.edu/legalcontent)
X. **HOSTING POLICY**

“Hosting” is defined as providing network access to a site, or network accessible location, which provides distribution of Content. Hosting of such distribution sites for entities other than University units, University affiliates, or registered student organizations (e.g., professional associations, consortiums, or journals) may be provided on University servers only when the entity has a relationship with the University that supports the University’s teaching, research, or service mission. Such a relationship may be demonstrated by one or more of the following:

1. The entity is an organization of which the University itself is a member;
2. The entity is an organization of which a faculty or staff member is a member, and the appropriate University vice president having authority approves the hosting as being in support of the University’s teaching, research, or service mission; and/or
3. The University has, or enters into, an authorized contractual relationship for hosting the entity’s site.

The hosting of other distribution sites on or through the IT Resources by any User is strictly prohibited unless expressly authorized in writing by the University. This Hosting Policy, as part of the IT Policy, particularly applies to the hosting on or through the University’s IT Resources of any website or other site or network access point accessed by other Users, or third parties from outside of the University community, which serves to distribute any Content through any number of networking protocols.

Thus, User setup and maintenance of distribution access points on the IT Resources that employ such protocols are violations of the IT Policy, unless otherwise provided for above. Such protocols include, but are not limited to, HyperText Transfer Protocol, File Transfer Protocol, Simple Mail Transfer Protocol, Internet Relay Chat Protocol, BitTorrent, or any other application layer protocols, now known or devised at anytime hereafter used to distribute Content, including the “secure” variations thereof.
XI. WIRELESS POLICY

Wireless networks use a finite and shared part of the radio spectrum. To ensure that all Users of the IT Resources have fair access to the University’s wireless networks, the University will regulate this Resource. Because the wireless infrastructure differs from the wired network, certain limits on bandwidth will be maintained. Accordingly, the University reserves the right to limit and restrict access to the wireless airspace on campus.

In order to ensure such reliable access to the wireless network, air space must be free of devices that could cause interference. The airspace on the University campus will be monitored for interfering devices. Accordingly, no User, or other community member, may install their own wireless access point, or any other device that interferes with the wireless-related IT Resources, on any University campus. Should any such device be found, the University will notify the party of the issues concerned with the use of that device and require it to be removed and/or shut down.

The User Responsibilities and Statement of Prohibited Uses and other obligations and prohibitions found elsewhere in this IT Policy, which govern the wired network portion of the IT Resources, also apply to the wireless network portion. Violations shall be handled in keeping with the guidelines set forth in the IT Policy and other applicable statutes and policies.
XII. INTERNET USAGE POLICY

Social networking (e.g. maintaining an account or presence on the likes of Facebook, MySpace, etc.) and the posting of web-logs (“blogs”) are increasingly popular forms of Internet usage. The University recognizes social networking and blogging as important means of self-expression and relationship networking. Moreover, the University notes the educational and professional benefits of both.

Nonetheless, Users who use social networking and blogs should be aware of certain issues. Most social networking pages and blogs can be viewed, or even added to, by any User or third party having access to the Internet. Accordingly, the University cautions each User against posting Content that could divulge the User’s private details or expose the User to embarrassment or ridicule. The University has no control over such potential disclosures by Users and, therefore, the University is not responsible for any such dissemination of private information.

The University reminds Users that, regardless of any efforts to the contrary, Users may be identified as members of the University community and therefore associated by third parties with the University. Accordingly, Users should remember that they are representatives of the University and should therefore comport themselves in accordance with the principles and standards of the University.

Moreover, every User should bear in mind that a potential employer, colleague, or other important business relation may review the User’s posted Content anywhere on the Internet that is publicly accessible. As such, no User should falsely state or exaggerate qualifications, accomplishments, affiliations, or other characteristics of either the User or the University.

Users should refrain from posting to social networks, blogs, or any other Internet site, any Content that may infringe any intellectual or other property rights of any other User or third party. The University disclaims any liability to User for User’s posting or submission of Content on the Internet, through use of the IT Resources, regardless of type of action brought against User.

Lastly, the University notes that it does not control the various third-party websites and other Internet destinations that Users access. Accordingly, the University expressly disclaims any liability to Users resulting from any damage to any computing resources owned or otherwise controlled by Users including, but not limited to, hardware, software, or any peripherals.
XIII. CORE GOOGLE SERVICES POLICY

Like social networking, the University recognizes that personal websites and groups are important means of self-expression and relationship networking, and can provide many educational and professional benefits.

Google Sites and Google Groups provide the opportunity to easily create and share webpages and information that are hosted outside the University’s own website. However, sites published via Google Sites using a Fordham email address will be identified with Fordham University within the websites URL. Similarly, groups created via Google Groups may also be identified with Fordham University. The Fordham logo may also be displayed. It is likely, therefore, that users of Google Sites and Google Groups (“Users”) will be identified as members of the University community and therefore associated by third parties with the University. Accordingly, Users should remember that they are representatives of the University and should therefore comport themselves in accordance with the principles and standards of the University.

Users should refrain from posting any Content that may infringe any intellectual or other property rights of any other User or third party. The University disclaims any liability to User for User’s posting or submission of Content on the Google Sites regardless of type of action brought against User.

Websites created with Google Sites will not be linked into or searched through www.fordham.edu, the main University Web Site.

Because your activity using Google Sites and Google Groups with a Fordham email address is governed by the agreement between Google and Fordham University, and will indicate your personal affiliation with Fordham, its use is governed by the following rules:

- You must abide by all terms of the IT Acceptable Use Policy, calling special attention to the sections regarding copyrighted material and cloud computing.
- The posting, storage, or disclosure of any Fordham Protected or Fordham Sensitive Data is strictly prohibited.
- Material presented must reflect the spirit and mission of the University and must not, in any way, be offensive or derogatory.
- In additional to abiding by these terms of use, you must also abide by the relevant rules and regulations that govern your classification (faculty, student or staff) within the University.

Failure to abide by the above rules may result in disciplinary action.
XIV. NON-CORE GOOGLE SERVICES POLICY

The University recognizes that “social networking” is an important means of self-expression and relationship networking, and can provide many educational, social, and professional benefits. Google has many tools available to the University community. Fordham University has an agreement in place with Google for Mail, Calendar, Drive, Sites and Groups. These are known as Google Core Services.

While there are many other Google products available by Google under the Fordham portal, including but not limited to Google+, YouTube, Picasa, Voice, Blogger, Wallet, and Cloud Print, use of these services are not covered by the agreement between Fordham University and Google. As such, by using any service that is not defined as a Google Core Service with your Fordham Gmail account, you are entering into a private agreement between yourself and Google, and you are not covered by the same protections as you would be using Fordham’s own systems.

However, users of non-Google Core Services may be identified with Fordham University because of their email address and other identifying information. Accordingly, Users should remember that while using these non-Google Core Services they are not representatives of the University and the University disclaims any liability to private use of these services, regardless of type of action brought against the user.

While Fordham does not regulate the private use of non-Google Core Services by members of the Fordham Community, the sharing posting, storage, or disclosure of any Fordham protected, sensitive, confidential or proprietary data on any social networking, including those offered by Google, or any other non-University venue is strictly prohibited.