Menu For Information Technology

IT Services

Standard Software

System Status

Project Requests

IT News and Events

About Us

User Responsibilities and Statement of Prohibited Uses

A. Spirit of Use

Only authorized users can access and use the University's IT Resources. Access and use are limited to purposes that are consistent with the University Code of Conduct and the instructional, research, and administrative goals and mission of the University.

All Users are expected to adhere to the University Code of Conduct when using IT Resources to communicate with others. Users are also bound by federal, state, and local laws relating, including, but not limited to, those relating to civil rights, harassment, copyright, security, and other applicable statutes relating to the use of IT Resources. Users are prohibited from using IT Resources for personal economic gain or in a manner that could jeopardize the University's tax-exempt status or violate the laws and regulations noted in the Government Relations Guide for Engaging Elected Officials.

B. User Names

The University recognizes that a common practice in computing, online or otherwise, involves using a username, login, or Fordham Username that may be different from the User's legal name.

Users may not use the IT Resources under any false name, identification, email address, signature, or other media. The University prohibits using the username or credentials of another person or entity without proper authorization.

C. Passwords and Authentication

Users should follow the guidelines below to prevent unauthorized access.

- Use a different password for each account;
- Use biometrics where possible (e.g., fingerprint, Apple™ Face ID, iris scan);
- Use passphrases (e.g., movie phrases, book quotes);
- Use long passwords (more than 12 characters);
- Do not write down your password(s) or store them in an unsecured manner;
- Your password must:
    - Be eight characters or more;
    - Contain at least one number;

    - Contain at least one uppercase and one lowercase character; and
    - Not contain any of the following special characters: "@," "&," or "/."
- Avoid using:
    1. Birth dates;
    2. Names (first, last, or any combination of your first and last names);
    3. Unaltered words that could be found in a dictionary on their own, including non-English words and words spelled backward;
    4. Telephone numbers;
    5. Social Security numbers;
    6. Fordham Identification Numbers (FIDN); and
    7. Alphabet or keyboard sequences (e.g., "QWERTY").
- All mobile devices that access IT Resources must be secured using a PIN (6-digit minimum) or other password protection;
- All mobile devices must enable automatic lockout for idle devices for (5) five or fewer minutes, where possible;
- All mobile devices must have remote wipe capability installed and enabled, where possible.

D. Additional Responsibilities

All Users must comply with the following:

- 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;
- All local, state, federal, and international laws;

- All applications and software license agreements are owned and managed by the University;
- The legal and educational standards of software use as published in the EDUCOM Code;
- The appropriate Fordham-provided email accounts are used in alignment with the appropriate role-based criteria per the Role-Based Email Accounts Policy;
- IT policies are listed in the IT Policies, Procedures, and Guidelines.

Users also are responsible for the following:

- Respecting authorial integrity and the intellectual property rights of others;
- Respecting and protecting the confidentiality, integrity, and availability of all University IT Resources;
- Backing up User's IT Resources, software, and data to appropriate backup storage systems per the Backup Policy;
- Backing up personal mobile devices, since the University does not accept liability for the maintenance, backup, or loss of data on those devices;
- Ensuring mobile device's security controls are not subverted via hacks, jailbreaks, security software changes, or security setting changes and working with the Service Desk to test and validate any configuration, application, or settings; and

Users of mobile devices that access IT Resources from non-Fordham-owned devices are expected to take reasonable measures to protect the security and integrity of that data, including:

- Following the rules in the Wireless Use Policy,
- Protecting the physical security of the device,
- Maintaining the software configuration of the device (i.e., operating system, installed applications),

- Installing an up-to-date and secure operating system and application software as they become available,
- Following the rules of Fordham Protected or Fordham Sensitive data per the Data Classification and Protection Policy and Data Classification Guidelines.

Users should note that the University is not liable for the loss, theft, or damage of any User's personal mobile devices, including, but not limited to, when the device is being used for University business or during business travel.

E. Additional Prohibited Uses

Users are prohibited from accessing or using IT Resources to:

1. Violate the University Code of Conduct, including University Regulations.
2. Send unauthorized mass mailings to newsgroups, mailing lists, or individuals, including, but not limited to, unsolicited commercial email (spam), floods, and bombs;
3. Give others unauthorized access to any User account or IT Resources;
4. Improperly use, interfere with, dismantle, disrupt, destroy, or prevent access to any portion of IT Resources;
5. Violate or compromise the privacy of other Users or third parties in violation of applicable law;
6. Disguise or attempt to conceal the identity of the account or other IT Resource being used, including spoofing resource addresses, impersonating any other person or entity, or misrepresenting an affiliation with any other person or entity (see the IT Anti-Spoofing Policy for more details);
7. Engage in wasteful use of IT Resources or unfairly monopolize them to the exclusion of others;
8. Interfere or degrade security controls of the IT Resources;

9. Exploit or otherwise use the IT Resources for personal gain or commercial purposes;
10. Use IT Resources for criminal or prohibited acts;
11. Violate any applicable local, state, federal, or international law; or
12. Knowingly, without authorization, run, install, upload, post, email, or otherwise transmit any computer code, file, or program, including, but not limited to, computer viruses, Trojan horses, worms, or any other malware, that negatively impact IT Resources.

Sections in Acceptable Uses of IT Infrastructure and Resources Policy

Need Help?

IT Service Desk

Fordham.edu/ITHelp

Online Support

Walk-In Centers

McShane Center 266 | RH

Leon Lowenstein SL18 | LC

Social Media

Follow us on X

Follow us on Instagram

Check out our Blog

718-817-3999

HelpIT@fordham.edu

View Our Walk-In Hours