Acceptable Use for FIT IT Systems

Policy IT001
Responsible Administrator: Vice President for Information Technology and CIO
Responsible Office: Office of the Vice President for Information Technology and CIO
Issued: April 2021

Policy Statement

Fashion Institute of Technology (FIT or the "college") provides a range of computing equipment, networks, and information resources ("FIT IT Systems") to support the instructional, research, and administrative functions of the college, as well as to enhance the well-being of the FIT community. This policy is intended to guide all Users of FIT IT Systems whether affiliated with FIT or not, accessing from campus or remote locations, on the acceptable use of FIT IT Systems. FIT IT systems shall be used for purposes that are legal, ethical, and consistent with FIT policies and the college's mission. Violations of this policy constitute unacceptable use of FIT IT Systems.

Reason for the Policy

This policy on the acceptable use of FIT IT Systems incorporates the ethical principles of respect and reverence for the rights of other individuals that are central to FIT's mission and identity. It supplements existing FIT policies and agreements, as well as local, state, and federal laws and regulations. It is the responsibility of all Users of FIT IT Systems to abide by this policy.

Who is Responsible for this Policy

- Division of Information Technology
- Data Owners

Who is Affected by this Policy

- All Users of FIT IT Systems

Definitions

- **Authentication** A security method used to verify the identity of a User.

- **Authorization:** The lawful and business-appropriate permission and access rights granted to a User.

- **Data Owners:** Vice Presidents or their designees who have planning and policy-level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.

- **FIT IT Systems:** All computer systems (including all computer programs, software, databases, firmware, and associated hardware, including fixed and mobile), servers, networks, endpoints,

electronic data, electronic communications, telecommunications, online and offline digital storage, that are owned, leased, administered, managed, maintained, supported, or otherwise provided by FIT.

- **Unauthorized Access:** Looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and/or legitimate business need.

- **User:** Any individual, authorized or not, using any FIT IT System from any location.

Principles

- **Acceptable Use:** Users may use only the FIT IT Systems for which they have authorization. Users must take reasonable precautions to prevent others from gaining Unauthorized Access to FIT IT Systems (see Information Security Policy). Each User is responsible for reasonably safeguarding their authentication credentials and is presumed responsible for all activities that originate from their authentication credentials and devices.

    - **Institutional Use:** Institutional use of FIT IT Systems must be for purposes that are consistent with FIT's mission, the User's legitimate business role within the college, and the policies and legal requirements (including license agreements and terms of service) of the college, and not for unauthorized commercial purposes.

    - **Personal Use:** Personal use of FIT IT Systems is acceptable when it does not interfere with the performance of college-related responsibilities, does not compromise the functionality or degrade the performance of FIT IT Systems, does not consume a significant amount of FIT IT Systems or resources, does not create unreasonable security risks for FIT IT Systems, and is otherwise in compliance with this policy and all applicable FIT policies.

    - **Unacceptable Use:** Use of FIT IT Systems must not violate applicable federal, state, and local law, including copyright laws, or applicable college policies, and, if travel is involved, the laws of the relevant nation or state. From any location, FIT IT Systems may not be used to transmit malicious, harassing, or defamatory content. FIT IT Systems may not be removed, or used in a way that disrupts or otherwise interferes with any college activities, or that is inconsistent with FIT's policies, without approval from the Division of Information Technology. Any action or attempt to circumvent FIT IT System safeguards, including hacking, cracking, phishing or similar activities, or the unauthorized use of another user's authentication credentials, is a direct violation of this policy.

    - **Political Use:** The use of FIT IT Systems shall be in accordance with the college policy on Political Election Activity and Legislative Advocacy.

- **Access and Privacy:** Wherever applicable FIT has the right to access, preserve, destroy, monitor, review, and restrict all FIT data stored on or transmitted through FIT IT Systems. Wherever applicable FIT has the right to perform maintenance (planned and unplanned) that may temporarily restrict access to FIT IT Systems (see Related Documents section for more information). The college endeavors to afford reasonable privacy for Users and does not access data created and/or stored by Users on FIT IT Systems except when it determines that it has a legitimate operational and/or legal need to do so. As a public institution, FIT is subject to state FOIL law and Users are reminded

all FIT data stored or transmitted through FIT IT Systems may be subject to disclosure through FOIL or other legal requirements.

- **Digital Millennium Copyright Act ("DMCA")**: The college is required to comply with the DMCA and reserves the right to temporarily or permanently terminate the network access of, or to take other disciplinary action against, Users who are found to repeatedly infringe the copyright of others. FIT reserves its rights under all applicable safe harbors of the Digital Millennium Copyright Act ("DMCA"). FIT shall appoint a designated agent to receive notices of claimed infringement under the DMCA, work with relevant FIT offices to respond to such notices expeditiously, including removing and disabling access to infringing material, and shall accommodate and not interfere with technical measures designed by copyright holders to identify and protect copyrighted works. Users are subject to termination of access as outlined in the Written Plan Addressing DMCA and Peer-to-Peer File Sharing. For all other copyright issues, please refer to FIT's Intellectual Property policy.

- **Disclaimer:** The college provides access to digital resources including but not limited to databases, forums, search engines, and the Internet. Where these materials are not affiliated with, endorsed by, or reviewed by FIT, the college takes no responsibility for the truth or accuracy of the content found within these sources and the college cannot protect individuals against the existence or receipt of material that may be offensive to them.

  FIT reserves the right to install spam, anti-malware, and spyware filters and similar devices if necessary in the judgment of FIT's IT Division to protect the security and integrity of FIT IT systems. FIT will not install filters that restrict access to e-mail, instant messaging, chat rooms or websites based solely on content, unless such content is illegal or otherwise violates college policy.

  FIT shall not be responsible for any damages, costs or other liabilities of any nature whatsoever with regard to the User or an authorized third party's use of FIT IT systems. This includes, but is not limited to, damages caused by unauthorized access to FIT IT systems, data loss, or other damages resulting from delays, non-deliveries, or service interruptions, whether or not resulting from circumstances under FIT's control.

Responsibilities

- **Users**: are required to adhere to this policy while using FIT IT Systems. Users are responsible for conducting themselves in a professional, responsible, and courteous manner at all times and should exercise good judgement regarding reasonable personal use. Users are responsible for ensuring any college records they manage are backed-up and accessible in accordance to the guidelines developed by their division/department administrators. (see Records Retention and Disposition Policy)

- **Supervisors:** in preparation for an individual's separation from the college or division/department, supervisors are expected to ensure that data is preserved if their functional area requires access to data or resources previously managed by the employee, and that copies of critical work product remain available to the department/division. (See Records Retention and Disposition Policy)

- **Data Owners:** in conjunction with the Division of Information Technology are responsible for the standards that determine authentication and authorization.

- **System Administrators:** monitor FIT IT Systems for misuse and promptly take action when an unauthorized access is detected.

- **Vice President and Chief Information Officer:** in consultation with the Office of the General Counsel and appropriate division/department administrators is responsible for the technology that supports authentication and authorization of all Users.

Procedures

- **Digital Millennium Copyright Act ("DMCA") Notice:** Upon receipt of a valid notice under the DMCA, the designated agent will work with relevant FIT offices (e.g., Enrollment Management and Student Success, Office of Human Resources Management and Labor Relations, Office of General Counsel) to respond to such notices appropriately and expeditiously, including removing and disabling access to infringing material, where applicable.

  FIT has designated the following official to serve as its designated agent for receipt of notices of infringement under the DMCA:

  Assistant Vice President for Information Technology, and Chief Security Officer
  Fashion Institute of Technology
  7th Avenue and 27th Street
  New York, NY 10001
  Phone: (212) 217-3415
  Email: cybersafe@fitnyc.edu
  Additional details regarding DMCA procedures are available in FIT's Written Plan Addressing DMCA and Peer-to-Peer File Sharing (see Related Documents).

Violations

By use of FIT IT systems, Users are taking full responsibility for compliance with this policy and, as a result of the intentional, or negligent, unauthorized use, or misuse, of FIT IT systems, in addition to any other disciplinary action that may be taken, Users may be subject to civil or criminal charges, penalties, fees, or fines. FIT may temporarily or permanently terminate access to FIT IT Systems provided to any User who is found to be in violation of this or any applicable FIT policy, federal, state, or local laws, including those Users who have repeatedly infringed on the intellectual property rights of others. Appropriate circumstances include, but are not limited to, where: (1) a User of FIT IT Systems has been found by a court of competent jurisdiction to have infringed the copyrights of a third party on multiple occasions; (2) multiple valid, effective and uncontested notices have been provided to FIT alleging facts that are a violation by the User of this policy, or (3) flagrant abuse of access to FIT IT Systems has occurred. FIT reserves the right, in accordance with its disciplinary procedures summarized below, to terminate access permanently, for specific amounts of time, and/or to condition future access on completion of imposed sanctions.

In addition to any other disciplinary action, known violators may be subject to criminal prosecution, civil liability, or both for unlawful use of any FIT IT system. In accordance with the Higher Education Act's provisions on unlawful peer-to-peer file sharing, FIT advises that its Users may be subject to criminal and civil liability by downloading or uploading copyrighted work without authority. 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 statutory damages up to $150,000 per work infringed. A court can, in its discretion, also

assess costs and attorneys' fees and order injunctive relief. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five (5) years and fines up to $250,000 per offense. For more information, please see the website of the U.S. Copyright Office at: www.copyright.gov.

If an individual has observed, or is otherwise aware of, a violation of this policy, they must report the violation to the appropriate college office(s) or division(s) as outlined below, which shall investigate the allegation and, if appropriate, refer the matter to college disciplinary officials and/or law enforcement authorities. Employees shall fully cooperate with FIT in any investigation of a User's use of FIT IT Systems.

Violations of college policy will be handled in accordance with the following:

- **Employees:**
  Employees covered by the Collective Bargaining Unit will be disciplined according to the Collective Bargaining Agreement, as well as relevant law and college policy. For non-bargaining employees, the Vice President for Human Resource Management and Labor Relations, or their designee(s), will review the violation and make a recommendation to the President for appropriate counseling and/or disciplinary action based upon relevant law and college policy.

- **Students:**
  The Dean of Students will review the violation and implement appropriate counseling and/or disciplinary action in accordance with the Code of Student Conduct.

- **Third Party or Contractor**
  Violations of FIT policies by third parties will be addressed by FIT senior leadership at its sole discretion and in accordance with the relevant policy, laws, and circumstances.

Related Policies

- Code of Student Conduct
- Employee Code of Ethical Conduct
- Information Security
- Intellectual Property
- Internet Privacy
- Nondiscrimination and Anti-Harassment
- Political and Election Activity and Legislative Advocacy
- Public Access to Records
- Records Retention and Disposition

Related Documents

- Disciplinary Procedures (28.28.0 of Collective Bargaining Agreement)
- Privacy and Terms of Use
- System Status (Maintenance Windows, Maintenance Announcements, and Unplanned Service Interruptions)
- Written Plan Addressing DMCA and Peer-to-Peer File Sharing

Contacts

- **Vice President & Chief Information Officer**
  Division of Information Technology
  (212) 217-3400