FLORIDA NATIONAL UNIVERSITY'S
ACCEPTABLE USE POLICY REGARDING
INFORMATION TECHNOLOGY & COMPUTER USE

(the "Policy")

(Note: The entirety of this Section 8 shall be referred to as the "Policy")

Purpose

To support the mission of the University and the needs of its students, faculty, and staff, by facilitating the use of information technology.

Policy Statement

The University acknowledges that information technology has many benefits, and in many instances is indispensable to an employee's and student's daily tasks. This Policy outlines the standards of acceptable use with respect to those information technology resources that are provided by the University. Inappropriate use of information technology can place the University and others at risk. By using any of the University's information technology resources, Users agree to abide by the Policy, in its current form and as amended from time to time. The current version of this Policy can always be obtained from University administration. All references in this Policy to "employees," "students," "users," "you," or "your" shall be to employees and/or students of the University, as applicable.

Compliance Statement

The University complies with all applicable federal, state, and local laws, and nothing contained herein is intended to be a violation of those rights and responsibilities. The terms of this Policy shall yield to applicable law where required. The University requires that all users act responsibly in using the Information Technology Resources, and do so in compliance with all applicable laws, administrative rules and regulations, all University policies, and all contractual and license agreements. Users are responsible for the appropriate use of the Information Technology Resources, and for taking reasonable precautions to secure all Information Technology Resources used by them. Users are responsible for reporting to administration malfunctioning equipment or applications, inappropriate uses of the Information Technology Resources, unauthorized activity, and any suspected or actual breaches of security, and are responsible for assisting in the resolution of such matters. Users are responsible for promptly reporting to the University in writing any suspicion or occurrence of any unauthorized activity (as outlined herein) as it may pertain to the Information Technology Resources. The duties and obligations imposed by this Policy shall be in addition to and not a limitation of any duties or obligations otherwise imposed by applicable law.

Agreement to the Policy

By using any of the Information Technology Resources of the University, Users expressly agree to strictly abide by the terms and conditions contained within this Policy, in its current form and as amended from time to time.

Definitions

1. The "University" or "FNU" shall refer to Florida National University.

2. "Information Technology Resources" shall refer to (but shall not be limited to) any and all University facilities, devices, peripherals, applications, services, networks, accounts, and resources used for or in connection with the University's processing, transfer, storage, access, and/or dissemination of information.

3. "Electronic Communication" shall refer to (but shall not be limited to) electronic mail, instant messaging, electronic messaging, social media communications, or any other form of communication transmitted through any of the Information Technology Resources.

4. "Data" shall refer to any and all information residing on or transmitted through the Information Technology Resources.

5. "Users" shall refer to those individuals authorized by the University to use the Information Technology Resources. The term "Users" shall expressly include all of the University's students, faculty, staff, employees, visitors, and guests.

Technology and Data Property of the University

All Information Technology Resources are the property of the University. All forms of Data produced by University employees on or with the Information Technology Resources are the property of the University, and are considered confidential and proprietary. Users are entitled to use the Information Technology Resources only for purposes related to their employment or studies at the University. The Information Technology Resources may not be used for personal business. All Information Technology Resources used while employed by the University must be returned to the University upon termination of employment, or earlier as may be determined by University administration, along with any passwords necessary for the University to continue using the respective Information Technology Resources, uninterrupted. Deleting and/or the inappropriate altering or sharing of Data, whether during or after employment by the University, is strictly prohibited.

No Expectation of Privacy

Users shall not have any expectation of privacy in connection with their use of the University's Information Technology Resources. The University expressly reserves the right to audit and monitor all Data, Electronic Communications, and use of all Information Technology Resources. All employee Electronic Communications (including but not limited to email, voicemail, and text messages) and Data transmitted through the Information Technology Resources are the property of the University and are not private or confidential to the employee transmitting or receiving

such communications. The University has the right to monitor and review all Electronic Communications transmitted through the Information Technology Resources at all times. Users are responsible for the content of their Electronic Communications. All employee Electronic Communications are considered the University's business records, and may be discoverable in the event of litigation. Notwithstanding anything contained in this Paragraph, the University reserves all of its respective rights with respect to its confidential, private, non-public, and/or proprietary Data.

Passwords and Access Control

Passwords must meet certain minimum guidelines. Serious damage can be done to the University and the Information Technology Resources if someone gets your password. Choose a difficult password (e.g., your password should not include your login ID, your name, your spouse's name, your partner's name, your child's name, your pet's name, or any other names commonly known to others, and it should not be a word pertaining to the University, your work, your studies, or an activity that you participate in or follow that is commonly known), keep it secret, and change it whenever you think it has become known to someone else. Do not write your password down where someone can find it, and do not send it over e-mail, text message, or any other communication. Do not share your password with anyone or let anyone else access your account. Do not log on to your computer if someone can see you typing in your password. Do not access anyone else's account. You will be prompted to change your password from time to time. Users are responsible for all actions taken with their respective passwords. Immediately report to University administration any known use by another of your account or password. Employees must leave their computers on at night, but reboot them each morning. If an employee uses a remote access program, and needs to leave their computer on, it must be locked and in a locked room.

DO NOT LEAVE YOUR COMPUTER UNLOCKED WHEN UNATTENDED. WHEN STEPPING AWAY FROM YOUR COMPUTER AT ANY TIME (EVEN IF FOR JUST A SHORT PERIOD OF TIME), MAKE SURE YOUR SCREEN IS LOCKED AND PASSWORD-PROTECTED. DO NOT RELY ON THE SCREENSAVER AUTOMATICALLY LOCKING YOUR COMPUTER AFTER A CERTAIN AMOUNT OF TIME.

IMMEDIATELY REPORT TO UNIVERSITY ADMINISTRATION ANY IRREGULARITIES, ALERTS, OR ERRORS FLAGGED BY YOUR COMPUTER. NO ONE FROM UNIVERSITY ADMINISTRATION WILL EVER ASK YOU FOR YOUR PASSWORD.

Prohibited Activities

Examples of prohibited activities in connection with the Information Technology Resources include, but are in no way limited to, the following (in no particular order):

(a) Accessing or attempting to access Information Technology Resources without the University's authorization;

(b) Accessing or attempting to access Information Technology Resources that are beyond a user's access rights, or are the private files of another;

(c) Sharing your login information, and/or using someone else's login information (login ID and/or password);

(d) Altering, damaging, attempting to alter or damage, or performing any act which reasonably could alter or damage any of the Information Technology Resources or the property of another (including but not limited to making changes to any computer or network settings, downloading or installing programs, or opening any device);

(e) Copying or moving any University Data without authorization from administration, except where such activity is directly connected to job-related duties (such as with copying/cutting and pasting information while working with a file);

(f) Transmitting, storing, or retrieving any sensitive, proprietary, and/or confidential University Data (or disclosing any University Data which is not otherwise public) outside of the University and/or to anyone not reasonably authorized to obtain such University Data;

(g) Intentional introduction or propagation of computer viruses or malicious code into or from the Information Technology Resources, using the Information Technology Resources to conduct or participate in a denial-of-service attack, or using the Information Technology Resources in a way that disrupts or degrades its use by others;

(h) Transmitting, storing, or retrieving media such as music and video, unless such activity is directly related to official University business or studies;

(i) Playing video games;

(j) Violating any local, state, or federal laws, or any administrative regulations or policies, or performing any act which is reasonably likely to result in the violation of same;

(k) Circumventing or attempting to circumvent security, access controls, content filters, firewalls, digital rights management, or encryption;

(l) Violating any software license agreements or committing software piracy;

(m) Operating, promoting, marketing, or maintaining a private business;

(n) Transmitting, storing, or retrieving any Data that is discriminatory, pornographic, racist, obscene, profane, harassing or bullying, or that is reasonably likely to be deemed by anyone as containing such content;

(o) Transmitting any email which contains a falsified or misleading header or header information, or an alias sender;

(p) With respect to any internet site (including but not limited to any social media site or platform), establishing any identity that purports to be or could reasonably be interpreted to be an official identity of the University, without the prior express written permission from University administration;

(q) Transmitting any communication that purports to be or could reasonably be interpreted to be an official communication of the University, without the prior express written permission from University administration;

(r) Installing or downloading software of any kind, except where approved in advance by University administration;

(s) Removing from the University's premises any Information Technology Resources (except for those users assigned laptop computers or other portable devices intended for such purpose);

(t) Deleting or altering University Data, except where such alteration is directly connected to job-related duties (such as with the editing of a file);

(u) Performing any act intended to, or reasonably likely to, circumvent security or access controls of the Information Technology Resources, or the systems of any other individual and/or entity, including but not limited to the possession or use of any software or hardware used or reasonably likely to be used for purposes such as analyzing network performance or security, circumventing or removing software copy protection, revealing or uncovering passwords, identifying or probing security holes or vulnerabilities, decrypting files without authorization or without the proper decryption key/password, or otherwise exposing or weakening computer security methods, etc.;

(v) Connecting any personally owned device or storage medium to any of the Information Technology Resources, except when connecting to a public University Wi-Fi access point solely for the purpose of obtaining internet access;

(w) Performing any fraudulent or illegal activities, including but in no way limited to: gambling, trafficking in drugs or weapons, participating in terrorist activities, participating in any pyramid or Ponzi schemes, or attempting or gaining unauthorized entry into any computer system, whether part of the Information Technology Resources or otherwise; and

(x) Using the Information Technology Resources in any manner that will not represent the University in a positive and ethical manner.

None of these provisions are designed or intended to curtail activities under Section 7 of the NLRA.

File Storage

Employees are responsible for safeguarding and saving their work and the Data that they produce, and must save all Data to the appropriate network drive and location. Employees may not retain any copies of Data on their local drive, on removable storage, or online. Unless expressly authorized to do so by administration, saving, copying, moving, or backing up University Data on any other storage medium (including, but not limited to, a desktop computer, laptop computer, a removable storage device, or online storage) is strictly prohibited. Students are responsible for safeguarding and saving their work and the Data that they produce. The University does not provide any storage, backup, or archival services for student Data.

Third-Party Providers

The University may store its Data (and any portion and/or backups thereof) on file storage that is located at a remote hosting, service, and storage facility (or facilities) maintained and controlled by a third-party provider (or third-party providers). However, the University reserves the right to maintain any such Data internally, in the University's sole and absolute discretion and without further notice.

Electronic Mail

Employees and students are provided with email accounts by the University. These email accounts are provided through a third-party hosting provider, and all information pertaining to these accounts (including the electronic mail messages themselves, along with any attachments) may be located at a remote location maintained and controlled by a third-party provider. By using an electronic mail account provided by the University, such users agree to the terms of use and privacy policy of the University's third-party providers.

Copyrights

Users shall respect all copyrighted works and shall not copy, disseminate, or transmit any copyrighted materials without the prior express written permission of the copyright holder. Removing or altering any copyright or other intellectual property notice is strictly prohibited.

Enforcement - No portion of this Policy may be waived by any University employee. The failure of the University to enforce any of the terms of this Policy, or to exercise any right herein, shall not operate to or be construed as a waiver or relinquishment of any of the University's rights hereunder, with respect to the same or further conduct. A violation of this Policy (or any portion of this Policy) shall be grounds for disciplinary action up to and including termination of employment (with respect to employees) or expulsion from the University (with respect to students), in the University's sole and absolute discretion, subject to all applicable laws.

Changes to this Policy - This Policy may be changed at any time by the University, and in a manner determined by the University. Once changed, the revised Policy shall immediately become the official Policy of the University with respect to the Information Technology Resources. The University will notify you when this Policy is amended, and it is your

responsibility to stay up to date on the most current version, which can always be obtained from University administration.

IF YOU HAVE ANY QUESTIONS ABOUT THIS POLICY, PLEASE ASK UNIVERSITY ADMINISTRATION FOR ASSISTANCE.