CLARK ATLANTA UNIVERSITY

Policy 14.7 Acceptable Use of Computer Equipment Policy

<table>
<tr><td colspan="3">CLARK ATLANTA UNIVERSITY</td></tr>
<tr><td>Policy and Procedures</td><td colspan="2">Subject: Acceptable Use of Computer Equipment Policy</td></tr>
<tr><td rowspan="2">Department:

Office of Information Technology and Communications (OITC)</td><td>Review Date:
06/04/20</td><td rowspan="2">Issued By:

Chief Information Officer</td></tr>
<tr><td>Effective Date:
06/15/2020</td></tr>
<tr><td>Distribution:

All University employees</td><td>Required Approval:

University President</td><td>No. of Pages:

5</td></tr>
<tr><td colspan="2">Signature: Original signed by George T. French, Jr., Ph.D.</td><td>Date: 06/15/2020</td></tr>
</table>

TABLE OF CONTENTS

14.7 Acceptable Use of Computer Equipment Policy – Clark Atlanta University

1.0 Policy Statement

The purpose of this policy is to outline the acceptable use of computer equipment at Clark Atlanta University. These rules are in place to protect the staff, faculty, partners and the University. Inappropriate use exposes Clark Atlanta University ("University") to risks including ransomware, virus attacks, compromise of network systems and services, and legal issues. When using University resources to access and use the Internet, users must realize they represent the University.

2.0.1 Procedures Narrative

2.0.2 General Use and Ownership

2.0.2.1 Clark Atlanta University proprietary information stored on electronic and computing devices whether owned or leased by Clark Atlanta University, staff, faculty, partners or a third party, remains the sole property of the University. You must ensure through legal or technical means that proprietary information is protected in accordance with the *National Institute of Standards and Technology Special Publication 800-171.*

2.0.2.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Clark Atlanta University proprietary information.

2.0.2.3 You may access, use or share Clark Atlanta University proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

2.0.2.4 Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the University in any way, not in breach of any term and condition of employment and does not place the individual or the University in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

2.0.2.5 For security and network maintenance purposes, authorized individuals within Clark Atlanta University may monitor equipment, systems and network traffic at any time, per *Clark Atlanta University 14.3 Information Security Policy*.

2.0.2.6 Clark Atlanta University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.0.2.7 Acceptable employees use of system and network resources shall align with the ethical guidelines established in the *Clark Atlanta University 2.4.0 Code of Ethical Conduct Policy*, whether on campus or working remotely.

2.1 Security and Proprietary Information

2.1.1 All mobile and computing devices that connect to the internal network must comply with *14.9 Remote Access Policy.*

2.1.2 System level and user level passwords must comply with the *14.5 Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

2.1.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

2.1.4 Postings by staff, faculty, and partners from a Clark Atlanta University email address to online media sites should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Clark Atlanta University, unless posting is in the course of business duties.

2.1.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

2.2 Unacceptable Use

The following activities in the following subsections are, in general, prohibited. Staff, faculty, and partners may be exempted by appropriate university leadership from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a staff, faculty, and partner of Clark Atlanta University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Clark Atlanta University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

2.3.1 System and Network Activities

The following activities are strictly prohibited, and shall not be granted an exception:

2.3.1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Clark Atlanta University.

2.3.1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Clark Atlanta University or the end user does not have an active license is strictly prohibited.

2.3.1.3 Accessing data, a server, or an account for any purpose other than conducting Clark Atlanta University business, even if you have authorized access.

2.3.1.4 Importing or exporting software, technical information, encryption software or technology in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.

2.3.1.5 Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

2.3.1.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

2.3.1.7 Using a Clark Atlanta University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and which conflict with the University's established policies.

2.3.1.8 Making fraudulent offers of products, items, or services originating from any Clark Atlanta University account.

2.3.1.9 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

2.3.1.10 Port scanning or security scanning where prior notification to the Office of Information Technology and Communications has not been made.

2.3.1.11 Executing any form of network monitoring which will intercept data not intended for the employee's host, where this activity is not a part of the employee's normal job/duty.

2.3.1.12 Circumventing user authentication or security of any host, network or account.

2.3.1.13 Introducing unapproved technology into the Clark Atlanta University network.

2.3.1.14 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

2.3.1.15 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

2.3.1.16 Providing information about, or lists of, Clark Atlanta University staff, faculty, and partners to parties outside Clark Atlanta University without proper authorization. Such requests should be forwarded to the Office of Planning, Assessment and Institutional Research (OPAR).

2.3.2 Email and Communication Activities

2.3.3 Whenever staff, faculty, and partners state an affiliation to the University, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the University." Questions may be addressed to the Office of Institutional Advancement.

2.3.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2.3.2.2 Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

2.3.2.3 Unauthorized use, or forging, of email header information.

2.3.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

2.3.2.5 Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

2.3.2.6 Use of unsolicited email originating from within Clark Atlanta University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Clark Atlanta University or connected via Clark Atlanta University's network.

2.3.2.7 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.3.2.8 Inappropriate use of communication methods for the purpose of promoting or supporting illegal activities, receiving or sending material that violates Clark Atlanta University policies against harassment or the safeguarding of confidential or proprietary information.

2.3.3 Blogging and Social Media

2.3.3.1 Blogging by staff, faculty, and partners, whether using Clark Atlanta University's property and systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Clark Atlanta University's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Clark Atlanta University's policy, is not detrimental to Clark Atlanta University's best interests, and does not interfere with an employee's regular work duties. Blogging from Clark Atlanta University's systems is also subject to monitoring.

2.3.3.2 Clark Atlanta University's Confidential Information policy also applies to blogging. As such, employees are prohibited from revealing any Clark Atlanta University confidential or proprietary information, trade secrets or any other material covered by Clark Atlanta University's Confidential Information policy when engaged in blogging.

2.3.3.3 Staff, faculty, and partners shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Clark Atlanta University and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by *Clark Atlanta University's 2.4.0 Code of Ethical Conduct Policy*.

2.3.3.4 Staff, faculty, and partners may also not attribute personal statements, opinions or beliefs to Clark Atlanta University when engaged in blogging. If a staff, faculty, and partner is expressing his or her beliefs and/or opinions in blogs, the staff, faculty, and partner may not, expressly or implicitly, represent themselves as a staff, faculty, partner or representative of Clark Atlanta University. Staff, faculty, and partners assume any and all risk associated with blogging.

2.3.3.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Clark Atlanta University's trademarks, logos and any other Clark Atlanta University intellectual property may also not be used in connection with any blogging activity.

3.0 Entities Affected by this Policy

This policy applies to staff, faculty, partners, contractors, consultants, temporaries, and other workers at Clark Atlanta University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the University. The use of the university's network and system resources is a privilege, not a right. This privilege can be revoked or amended when justified. Failure to comply with this policy may result in disciplinary action as outlined in established in *Clark Atlanta University's 2.4.0 Code of Ethical Conduct Policy.*