University of CINCINNATI	Policy Title: **Acceptable Use of University Information Technology Resources**	Policy Number: **9.1.3**
Category: Information Technology	**Effective Date:** 09/03/2021	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Faculty/Staff/Students/ Affiliates/Guests	**Prior Effective Date:** 09/25/2019	**Responsible Office(s):** Office of Information Security

Background

A trusted and effective information technology environment ("IT environment") is vital to the mission of the University of Cincinnati ("UC"). To that end, the university provides an IT environment which includes an array of institutional electronic systems, computing services, networks, databases and other resources (collectively, "IT resources" or "resources"). These resources are intended to support the educational and work activities of members of the university's academic community and their external collaborators, to support the operations of the university, to provide access to services of the university and other publicly available information, and to ensure a safe and secure IT operating environment to all members of the university community.

This policy is intended to define and promote the responsible use of information technology at the university while simultaneously limiting and preventing abuse of IT resources. Access to and usage of IT resources entails certain expectations and responsibilities for both individuals and managers of the IT environment. These are stated below.

Policy

1 Applicability

1.1. This policy applies to all individuals using university technology resources ("Individuals"), regardless of affiliation and irrespective of whether these resources are accessed from UC's campus or from remote locations. Individuals covered by the policy include (but are not limited to) UC faculty and visiting faculty, staff, students, alumni, affiliates, guests or agents of the

administration, external individuals and organizations accessing network services via UC's computing facilities.

1.2. Within UC's IT environment, additional rules will apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks and to the uses thereof, or to college/departmental workplaces, or to specific types of activities (collectively, "departmental rules"). Departmental rules must be consistent with this policy, but also will impose additional or more specific requirements or responsibilities on Individuals.

2 Purposes and Appropriate Uses

2.1. IT resources are provided for university-related purposes and not intended to hamper support for the university's teaching, research and public service missions, its administrative functions, student and campus life activities. The university owned data and information stored on electronic and computing devices whether owned or leased by the individual or a third party, remains the sole property of UC.

2.2. Individuals are granted access to IT resources for the purposes described in this policy. Use is limited to those purposes, subject to Section 2.3

2.3. Incidental Personal Use

2.3.1. Individuals may make incidental personal use of IT resources, provided that such use is subject to and consistent with this policy, including Article 3 of this policy. Incidental personal use is the use of information technology resources by Individuals in support of activities that do not relate to their university employment or studies or to other activities involving and approved by the university. If personal use adversely affects or conflicts with university operations or activities, the Individual will be asked to cease those activities. In addition, incidental personal use of IT resources by an Individual may not interfere with the fulfillment of that Individual's job responsibilities or disrupt the work environment. Incidental personal use that inaccurately creates the appearance that the university is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

2.3.2. Individuals who make incidental personal use of IT resources do so at their own risk. The university cannot guarantee the security or continued operation of any IT resource or the security of any data.

2.4. The university purchases and maintains enterprise collaboration, social media, learning, research and other technology platforms. Whenever possible, faculty should leverage these enterprise tools available to them through the university learning management ecosystem. The use of enterprise tools reduces the risk to the university and increases compliance with university policies, procedures, standards and guidelines, and applicable regulatory requirements.

3 Individual Responsibilities

3.1. When an Individual accesses university computing services and accepts any university issued computing accounts, they agree to comply with this and all other related policies. All members of the university community are responsible for familiarizing themselves with any applicable policy prior to use.

3.2. Use of Resources Accessed through IT Resources

3.2.1. When using IT resources or resources owned by third parties that are accessed using IT resources, Individuals must comply with all applicable federal, state laws and local laws, all applicable university rules, ordinances, policies, and the terms of any contract or license which governs the use of the third-party resource and by which the Individual or the university is bound.

3.2.2. Intellectual honesty is of vital importance in the academic community. Individuals must not utilize IT resources to violate copyright, patent, trademark, other intellectual property rights, or engage in plagiarism.

3.3. Individuals will not engage in unauthorized use of IT resources, regardless of whether the resource used is securely protected against unauthorized use. Individuals will use only the computers, computer accounts and data for which they have authorization.

3.3.1. Use of equipment or devices that may negatively impact security, stability or performance of the university computing environment is prohibited, see the Network Device Standard.

3.4. Access of files belonging to another Individual.

3.4.1. Permitted access to another Individual's files or e-mail due to supervisory or other status does not entail access to the other Individual's personal and private information stored in the same location. Unauthorized use by an Individual of another Individual's personal identity or access (log-in) credentials is prohibited, as is sharing

of credentials between two or more Individuals per the university Password Policy.

3.5. IT resources will not be used to fund raise, advertise or solicit unless that use is approved in advance by the university. This prohibition does not include any UC campus union activity and any UC Foundation activity.

3.6. Political Activities

3.6.1. The rights of free expression and academic freedom apply to the use of University Information Technology Resources; so, too, however, do the responsibilities and limits associated with those rights. All who use the IT resources must act responsibly, in accordance with the highest standards of ethical and legal behavior.

3.6.2. Employees are prohibited from using IT resources in any way that would suggest institutional endorsement.

3.7. IT resources will not be used to operate a business or for commercial purposes unless that use is approved in advance by the university.

3.8. IT resources will not be used to support the operations or activities of organizations that are not affiliated with the university unless that use is approved in advance by the university.

3.9. Legal compliance

3.9.1. All members of the university community must obey:

3.9.1.1. All relevant federal, state and local laws. These include laws of general application, such as libel, copyright, trademark, privacy, obscenity, export control, as well as laws that are specific to computers and communication systems, such as the Computer Fraud and Abuse Act (CFAA) the Federal anti-hacking statute that prohibits unauthorized access to computers and the Electronic Communications Privacy Act (ECPA), currently under review by the Senate Judicial Committee to update the 1986 legislation especially with regards to digital due process and timelines.

3.9.1.2. All relevant university rules and regulations. These include the Rules of the University, the Student Code of Conduct, the various collective bargaining agreements between the university and its employees and all other university policies.

3.9.1.3. All contracts and licenses to the resources made available to the Individuals through the use of university information technology.

3.9.1.4. This policy, as well as other policies issued for specific systems.

3.9.1.5. All other applicable laws and regulations.

3.10. In operating its IT environment, the university expects Individuals to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched and employing security measures on their personal devices. Additional measures are described in the Data Governance & Classification Policy, Password Policy, Vulnerability Management Policy and other policies approved and posted on the Office of Information Security (OIS) website.

3.11. Exporting software, technical information, select research data, encryption software or technology, to a location outside of the United States in violation of international or regional export control laws, is illegal. The Export Controls Office must be consulted prior to export of any material that is in question.

3.12. Personal devices must not disrupt university services or bypass university established controls and safeguards.

4 Reporting and Enforcement

4.1. An Individual's access to IT resources may be limited, suspended or terminated without warning if that Individual violates this, or any other university policy. Alleged or suspected violations of this policy will be addressed by OIS and referred to the appropriate UC department.

4.2. OIS reserves the right to remove or disconnect any device from university information technology resources if such device negatively impacts, or has the potential to negatively impact, university operations, as determined by OIS and later reviewed with the corresponding unit management.

4.3. Investigations of information technology systems or services misuse is limited only to OIS, or their designee.

4.4. In addition to its own administrative review of possible violations of this policy and other university policies, the university is obligated to report certain uses

of IT resources to law enforcement agencies.

4.5. Individuals who violate this policy, other university policies or external laws may also be subject to disciplinary action and other penalties. If an investigation involving review of the content of a faculty member, staff member or student's files is required, authorization will be obtained from the Office of General Counsel or other appropriate departments, as necessary. Disciplinary action for violation of this policy is handled through the university's normal student and employee disciplinary procedures and through unit heads, human resources, Office of General Counsel, UCPD and Office of University Judicial Affairs, as documented in the Student Code of Conduct and other applicable departments and documents.

4.6. If OIS determines that an Individual has violated this policy, suspension, removal or disabling of the Individual account may occur. OIS will temporarily suspend or deny an Individual's access to IT resources when it is determined that such action is necessary to protect such resources, the university, or other Individuals from harm.

4.7. Anyone who becomes aware of a possible violation of this policy, other applicable policies or the more specific regulations of the systems that comprise IT resources must notify OIS immediately.

5 Security and Operations

5.1. The university may, without further notice to Individuals, take any action it deems necessary to protect the interests of the university and to maintain the stability, security and operational effectiveness of IT resources. Such actions may be taken at the institutional or local level and may include, but are not limited to, scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns and other uses of its information technology and block of unauthorized access to and unauthorized uses of, its networks, systems and data. Additionally, OIS may investigate based on the request of Office of General Counsel, UCPD, Human Resources, Office of Student Conduct and Community Standards, Research Integrity Officer, Office of Internal Audit, IT@UC leadership, Senior VP of Administration and Finance, Provost or Office of the President.

5.2. Undetermined abnormalities in system, service, individual or network behavior can be investigated by OIS to determine implications on university resources. If a violation of any applicable laws, regulations or policies is discovered during such an investigation, OIS will contact other appropriate

university departments for further follow-up.

6 Privacy

6.1. General Provisions

6.1.1. Responsible authorities at all levels of the IT environment will perform management tasks in a manner that is respectful of individual privacy and promotes Individual trust.

6.1.2. IT@UC may access Protected Health Information (PHI) as necessary in support of the university's health care components. IT@UC is a covered unit named in the university's HIPAA Policy.

6.1.3. Monitoring and Routine System Maintenance

6.1.3.1. The university will access IT resources as necessary for system maintenance, including security measures. The Network Operations Center (NOC), OIS and formally designated IT managers are authorized to monitor network traffic for malicious activity, suspicious patterns and in the course of investigation. Additional campus IT administrators can be approved to access and monitor specific traffic on specific networks for which they are responsible. Authorization must be obtained from OIS. The individual(s) must also complete a Non-Disclosure form and undergo a standard background check, if not already completed. Authorized personnel must demonstrate a need for and an understanding of the operation of network monitoring devices.

6.1.3.2. The university's routine operation of IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic and perform other essential administrative tasks. OIS may store incident related data as required. OIS may store aggregated data and usage logs for operational, compliance and statistical purposes.

6.1.3.3. No authorized personnel will use network monitoring devices to monitor employee electronic transmissions, conduct network scans, or access individual data for job performance evaluation, or as part of an unofficial investigation, without first receiving approval from OIS. This requirement is not intended to interfere with routine operations of staff who are required

to perform monitoring services to maintain the availability and integrity of the IT infrastructure.

6.1.4. The university may be compelled to disclose Individuals' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation and requests for public records under the Ohio Public Records Law or by request of the Office of General Counsel.

6.1.5. The university may disclose, at the Office of General Counsel discretion, the results of any general or individual monitoring or inspection of any Individual's record, account or device to appropriate university authorities and law enforcement agencies. The university may also use these results in its disciplinary proceedings.

6.2. Provisions Regarding Inspections and Disclosure of Personal Information

6.2.1. The university will never disclose contents of communications to an outside entity unless formally instructed to do so by the Office of General Counsel and:

6.2.1.1. When so required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the Individual or without the Individual's consent, as determined by the Office of General Counsel

6.2.1.2. In connection with an investigation by the university or an external legal authority into any violation of law or of any university policy, rule or ordinance. When the investigational process requires the preservation of the contents of an Individual's electronic records to prevent their destruction, the Office of General Counsel may authorize such an action.

6.2.1.3. If appropriate university personnel determine that access to information in an employee's electronic account or file is essential to the operational effectiveness of a university unit or program and the employee is unavailable or refuses to provide access to the information.

6.2.1.4. If the university receives an appropriately prepared and presented written request for access to information from the lawful representative of a deceased or incapacitated Individual.

6.2.2. If the university must use or disclose personally identifiable information about Individuals without their consent to protect the health and well-being of students, employees, or other persons in emergency situations, as formally instructed by UCPD, or to preserve property from imminent loss or damage, or as instructed by Office of General Counsel, to prosecute or defend its legal actions and rights.

Definitions

IT Environment or **IT Resources -** The broad range of technology services and devices available at the university and includes, but is not limited to, hardware, software, cloud and network resources.

Personal device - Any electronic device that is owned by a student, staff, faculty, or guest that is being used to access the university's IT resources.

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

Related Links

Board Rule 10-17-01 Conduct and Ethics: Statement on Political Policy
Board Rule 10-17-04 Conduct and Ethics: Use of University Resources
Data Governance & Classification Policy
FERPA Reference Guide for Faculty
HIPAA Policy
Human Resources Policies and Procedures
Network Device Standard
Password Policy
Student Code of Conduct
Vulnerability Management Policy