**UP09-001: Information Technology Resources Policy**
**Responsible Executive: Chief Information Officer ("CIO")**
**Responsible Office: Office of the CIO**
**Related Policy: UP09-002 Sensitive Data & Security Policy**
**Approval/Effective Date(s):**
**Revision Date:**
**Schedule Review Date:**

## I. POLICY STATEMENT

John Carroll University provides information technology resources to allow faculty, staff, and students to pursue the University's educational mission, which includes teaching, learning, service, research and administration. Thus, Information Technology Resources ("IT Resources"), as defined in this policy, must be used in a manner that furthers the University's mission.

Any access or use of information technology resources that conflicts with this Information Technology Resources Policy ("Policy" or "IT Policy") or any other University policy is not acceptable and will be considered a violation of this Policy. Additionally any activity that interferes, interrupts, compromises, or conflicts with the safe and efficient use of IT Resources is considered a violation of this Policy.

This Policy shall apply to all Users including, but not limited to, students, employees (faculty and staff), guests, affiliates, vendors and independent contractors. Use of IT Resources, even when carried out on a privately owned computer that is not managed or maintained by the University, is governed by this Policy.

This Policy supersedes any existing policies and procedures that are in conflict with the terms of this Policy.

## II. PURPOSE

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic mission and purpose of the University in teaching, learning, service, research and administration, and to ensure compliance with all applicable laws. It also provides notice, to all who use and manage IT Resources, of the University's expectations and regulations.

## III. SPIRIT OF USE

Users are responsible for the protection of University assets and for the accuracy, integrity and confidentiality of the information to which they have access. Users are expected to uphold the standards and principles of the University while using IT Resources. Accordingly, Users are prohibited from using any portion of IT Resources to post or transmit any information, Data, text, file, link, software, chat, communication or other content that is harmful, abusive, discriminatory, hostile, combative, threatening, insulting, embarrassing, harassing,

intimidating, defamatory, pornographic, obscene, or which negatively affects the University, another User, or any third party. Users who do not respect this Spirit of Use may be held in violation of this IT Policy.

## IV. DEFINITIONS

**A. Data**. All information that is used by or belongs to the University, or that is processed, stored, posted, maintained, transmitted, copied on, or copied from IT Resources.

**B. Functional Unit(s)**. The department, office, operating division, program, vendor, entity or defined unit of the University that has been authorized to access or use IT Resources.

**C. IT Resource(s)**. University information technology resources and services, including but not limited to computing, networking, communications and telecommunication systems, infrastructure, hardware, software, Data, records, Databases, personnel, procedures, physical facilities, and any related materials and services.

**D. User**. Any indiv**i**dual who uses accesses or otherwise employs, locally or remotely, IT Resources, whether individually controlled, shared, stand-alone, or networked, and with or without authorization, is considered a User under this Policy.

**E. Sensitive Data**. Data designated as private or confidential by law or by the University. Sensitive Data includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), research Data, trade secrets, classified government information, proprietary information of the University or any Data that could harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally. Sensitive Data shall not include records that by law must be made available to the general public.

## V. POLICY ELABORATION

**A. Access**. Access to some IT Resources is restricted to specific positions or units as determined by the appropriate functional unit head. Functional unit heads should determine and authorize the appropriate degree of access for each member of their units, and should provide unit members with adequate orientation and training regarding the appropriate use of all IT Resources. Using IT Resources outside of the scope of access granted by the University or attempting to exceed restrictions on access is a serious violation of this Policy and may potentially lead to criminal prosecution.

**B. Technical and Content-Based Restrictions**. The University reserves the right impose technical restrictions on the access to its network in ways that may disrupt the ability to utilize certain devices, programs, and protocols. Additionally, the University expressly reserves the right to impose content-based restrictions on the use of its IT Resources. Such restrictions may be necessary to protect the University and its constituents. The University recognizes that academic freedom and the freedom of inquiry are important values that may be hindered by an overzealous restriction of content. Therefore,

any content-based restriction scheme imposed on IT Resources will require appropriate Vice President authorization.

**C. Access Codes**. Users must take precautions to prevent unauthorized use of their access codes (passwords). Users will be held accountable for all actions performed under their access codes, including those performed by other individuals as a result of negligence in protecting the codes.

**D. Privacy**. Users are obligated to respect the privacy that other Users have in their own systems, Data, and accounts. Thus, it is a violation of this Policy for any User to engage in electronic "snooping," or to employ IT Resources for the purpose of "prying into" the affairs of others, i.e., to access or attempt to access electronic files, or to install/utilize image/audio recording devices, without proper authorization to do so for genuine business purposes of the University.

Users should be aware that the University cannot guarantee the security and privacy of IT Resources, as their uses may not always be completely private. For example, issuance of a password or other means of access is to assure appropriate confidentiality of University-related information and files. It does not guarantee privacy in all cases, especially for personal or unlawful use of IT Resources.

University may monitor IT Resources to ensure that they are secure and being used in conformity with this IT Policy and other University guidelines. The University, to the extent allowed by applicable law, reserves the right to examine, use, and disclose any Data found on the University's IT Resources for the purposes of furthering the health, safety, discipline, security, or property rights of any other User, person, or entity. Any Data that the University gathers from such permissible monitoring or examinations may also be used in disciplinary actions.

**E. Sensitive Data**. IT Resources containing Sensitive Data should be restricted based upon a need to know basis and should be guarded against both internal and external breaches. Thus, IT Resources containing Sensitive Data protected under either state or federal law should be controlled and protected in a manner that meets all pertinent legal requirements. Any breaches in the security and confidentiality of Sensitive Data must be reported in conformity with applicable legal and ethical obligations. IT Resources containing Sensitive Data must be collected, protected, accessed and managed consistent with the University's Sensitive Data & Security Policy, UP09.002. To the extent there is any uncertainty as to whether any Data constitutes Sensitive Data, it shall be treated as Sensitive Data until a determination is made by the CIO and Functional Unit head, in consultation with the University's General Counsel.

**F. Violation of Law**. Users are responsible for respecting and adhering to University policies and to local, state, and federal laws. Any use of IT Resources in violation of civil or criminal law at the federal, state, or local levels is prohibited. Examples of such use includes but is not limited to: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; exceeding authorized access; and making bomb or other threats.

In the event the University has reasonable suspicion that a User has violated any civil or criminal law, this IT Policy, or any other University policy, procedure, or regulation, the University reserves the right to access, inspect, monitor, remove, take possession of, or surrender to civil or criminal authorities the offending content, with or without notice or consent of the User. The University may also do so for the purpose of satisfying any law, regulation, or government request.

**G. Intellectual Property Rights**. The University takes the issue of intellectual property and similar rights seriously. Accordingly, the University requires every User to adhere to a strict policy of respecting intellectual property rights.

**1. Copyright**. With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). All copyrighted information, such as text and images, retrieved from IT Resources or stored, transmitted or maintained with IT Resources, must be used in conformance with applicable copyright and other laws. Copied material, used legally, must be properly attributed in conformance with applicable legal and professional standards.

**2. Software**. Software may not be copied, installed or used on IT Resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (including installation, use, copying, number of simultaneous Users, terms of the license, etc.) must be strictly followed. All software licensing is administered under the auspices of ITS.

**3. Fair Use**. The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

**4. Ownership**. All IT Resources developed by University employees, students, and contractors for use by the University, or as part of their normal employment activities, are considered "works for hire." As such, the University is considered the "author" and owner of these resources. This Policy does not alter the University's position or policy on intellectual property ownership for faculty and research Data.

**5. Reporting Infringement**. It is the responsibility of every User to avoid infringing any intellectual property right and to report the infringement of another User if and when it is discovered. Failure to respect such rights, or report infringements, is a violation of this IT Policy and subject to appropriate sanctions.

**H. Malicious Software**. It is the responsibility of all Users to take appropriate precautions against malicious software and to avoid actions or activities that may introduce or spread such software. It is also the responsibility of all Users to comply with University procedures designed to protect IT Resources against malicious software.

**I. Backups**. It is the responsibility of the User to ensure regular backup of Data stored on their individual computers and/or storage media. Backups are to be stored in a location that is physically secure and that protects the confidentiality of the Data. To avoid loss by fire or theft, backups of Sensitive Data must not be stored in the same locations as the original sources.

**J. E-mail Retention**. In order to maintain Data security, allow the University to administer IT Resources policies, and fulfill applicable legal obligations, all employees must use their JCU provided

and administered e-mail system and clients (currently MS Exchange, MS Outlook, Webmail, and Mirapoint) when conducting University business. The University maintains an e-mail retention period of 6 weeks. Users are required to retain Data with lasting value that is in their email inbox, and such Data must be maintained separate from e-mail files by creating copies elsewhere. Even though email backups are only retained for 6 weeks, recent backups may contain historic email data going back many months (or even years) unless you have deleted that information since the last backup. E-mail backups are maintained by ITS solely for disaster recovery purposes and thus all e-mail server backups are deleted after 6 weeks. It is the responsibility of each User to ensure that their Data retention conforms to the University's retention policies. Users must immediately suspend the routine destruction of all e-mail and other Data upon receipt of a litigation hold directive.

**K. Physical Security**. Users are responsible for the physical security of IT Resources assigned to them. Functional unit heads must ensure appropriate physical security by instituting and enforcing adequate policies and procedures governing entrance locks and/or for the use of the security devices made available by the University for the protection of equipment. Adequate power regulators and surge suppressors should be employed. Users are responsible at all times for the physical security of portable computers/devices that may be assigned to them.

**L. Use Inconsistent with University's Non-Profit Status**. The University is a non-profit, tax-exempt organization, and as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, IT Resources may not be used for personal commercial purposes, soliciting, or outside political campaigning by Users. Use of IT Resources in a way that suggests University endorsement of any political candidate or political initiative is also prohibited. Users must refrain from using IT Resources for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with an authorized University official.

**M. Reporting Suspected Violations**. Users have an obligation to report suspected violations of the IT Policy as well as any potential security or other breach of any portion of the IT Resources. Suspected violations of this Policy are to be reported to the CIO, the appropriate Functional Unit head, and the Office of Human Resources.

**N. Sanctions**. Failure to adhere to these policies can result in the suspension of IT Resources privileges, disciplinary actions and prosecution under state and federal laws when applicable. The University may restrict or suspend User privileges pending investigation and determination of the alleged violation(s). In the event of restriction or suspension of IT Resources privileges, a reasonable effort will be made to accommodate the academic IT Resources needs of the User during the investigation. University sanctions are imposed by the appropriate University authority and may include reimbursement to the University for the IT Resources, services and personnel charges incurred in detecting and proving the violation as well as from the violation itself. Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident.

**O. Non-Waiver**. A failure to enforce any provision of this policy does not constitute a waiver of said provision or an implied endorsement of any activity that would otherwise conflict with this policy.