John Carroll University

Header

Policy Name and Number: **Acceptable Use Policy** (JCU-IT-POL-101)

Policy Developer(s): Information Technology Services

Original Date: August 2, 2010

Approval Date: May 25, 2017; October 18, 2022 (interim); ; May 2, 2024

Contact Person for Website: Director of IT Security

Body

POLICY

John Carroll University provides Information Technology ("IT") 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, as defined in this policy, must be used in a manner that furthers the University's mission.

Any access or use of IT Resources that conflicts with this 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.

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.

SCOPE

This Policy shall apply to all Users including, but not limited to, students, employees (faculty and staff), volunteers, guests, affiliates, vendors and independent contractors who use IT Resources.

PROCEDURES

Use of University 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.

Users of IT Resources are subject to applicable federal, state and local laws, applicable contracts and licenses, and other University policies, including Human Resources policies, and those contained in the Faculty Handbook and Student Community Standards, including but not limited to those related to copyright and intellectual property compliance.

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 penalties and/or appropriate corrective action under University policies. For more information, reference Policy 106 Identity and Access Management.

B. Technical and Content-Based Restrictions. The University reserves the right to 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, including but not limited to restrictions necessary related to safety considerations, unlawful activity, or use that violates other University policies. 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 Credentials. Users must take precautions to prevent unauthorized use of their access credentials, including, but not limited to, user ids, passwords, passphrases, and tokens. Users will be held accountable for all actions performed under their access-credentials, including those performed by other individuals as a result of negligence in protecting the codes. See Policy 106 Identity and Access Management Policy for further detail.

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 or other devices to access or attempt to access electronic files, or to install/utilize image/audio recording

devices, without proper authorization to do so for legitimate business purposes of the University.

1. 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.

2. University may monitor IT Resources to ensure that they are secure and being used in conformity with this IT Policy and other University policies and 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 corrective action processes. Monitoring or access of information on IT Resources will be conducted under the direction of IT and/or the CIO, in consultation as appropriate with the Office of Legal Affairs and/or other appropriate senior leaders.

E. Sensitive Data. IT Resources containing Sensitive Data should be restricted to those with a need to know 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 policies. 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, Cybersecurity Program Officer, and/or Functional Unit head, in consultation with the University's General Counsel. See Policy 100 Sensitive Data and Cybersecurity Policy for additional details.

F. Violation of Law. Users are responsible for complying with University policies and 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 or obscene materials; receiving, transmitting, or possessing child pornography; infringing

copyrights or other intellectual property; 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 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 and related IT Resources, 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 that prohibits violation of 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 (i.e., "fair use" of certain materials in a classroom setting, for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

H. Ownership. All IT Resources are the property of the University. 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, as described in the Faculty Handbook.

I. 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.

J. 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. The University provides antivirus/anti-malware protection for University-provided computing assets, including PC workstations, laptops, and servers. Users are required to provide similar industry-accepted antivirus/anti-malware protection for their own devices.

K. 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.

L. Data Retention and Requirement for Use of University Gmail. 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 JCU-administered Gmail address when conducting University business. Users may not automatically distribute or forward Sensitive Data to external, non-JCU email accounts, and the University reserves the right to place technical restrictions upon such sharing or forwarding. Although Gmail provides some recovery capability for deleted files, that recovery capability is time-limited and cannot be guaranteed. Users are required to retain Data with lasting value separately from email files by creating copies elsewhere. Email may be retained indefinitely by the Gmail system unless Users have deleted that information. It is the responsibility of each User to ensure that their Data retention conforms to their functional unit's retention policies. Users must immediately suspend the routine destruction of all email and other Data upon receipt of a litigation hold directive from the Office of Legal Affairs or IT.

M. 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.

N. Use Inconsistent with the University's Non-Profit Status or University Policy. 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 campaign or lobbying activities 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.

The University reserves the right to take appropriate action under this policy or other corrective action or disciplinary processes if a User posts online or on social media—using statements, photographs, video, audio, or other content that reasonably could be viewed as: 1) malicious, obscene, threatening or intimidating; 2) disparaging to other employees, students, or visitors, or 3) that constitutes harassment, discrimination, or bullying. Examples of such conduct might include offensive posts meant to intentionally or negligently harm someone's reputation or posts that could contribute to a hostile learning, living, or work environment on the basis of race, sex, disability, age, religion or any other status protected by law or University policy. This section is not to be construed as prohibiting either speech protected by law, including the National Labor Relations Act, or faculty speech protected by Academic Freedom, as described in the Faculty Handbook.

O. 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.

P. Sanctions. Failure to adhere to this policy and other policies related to the use of IT Resources may result in the suspension of IT Resources privileges, disciplinary and corrective actions and criminal prosecution and penalties 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.

Q. 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.

R. Web Browsing and Internet Usage. The Internet is a network of interconnected computers over which JCU has very little control. The User must recognize this when using the Internet, and understand that it is a public domain and the User can come into contact with information, even inadvertently, that the User may find offensive, sexually explicit, or inappropriate, or that may be illegal in some jurisdictions. Users must use the Internet at their own risk. JCU is specifically not responsible for any information that the User views, reads, or downloads from the Internet. Access to the Internet is provided to Users in order to perform certain aspects of their education or jobs. The University reserves the right to monitor, review, access, and control all Users' network usage at all times, with or without notice. Users have no expectation of privacy regarding sites visited or material downloaded.

1. *Personal Use.* JCU recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of JCU IT Resources to access the Internet is permitted as long as such usage complies with applicable provisions elsewhere in this document and does not have a detrimental effect on JCU operations, other Users, or, if employed by JCU, on the User's work performance.
2. *Peer-to-Peer File Sharing*. Peer-to-Peer (P2P) file-sharing/networking applications (examples include, but are not limited to, Ares Galaxy, Vuze, Limewire, uTorrent, BitTorrent, eMule, Shareaza, Frostwire) are not allowed on the JCU IT Resources under any circumstance. Students may use this technology on JCU IT Resources so long as it does not violate any other part of this policy such as prohibited illegal activities.

S. Blogging. Blogging by JCU's employees is subject to the terms of this policy, whether performed from JCU IT Resources, personal systems, or other external systems. The User is asked to recognize that information posted on a blog immediately becomes public information and thus to exercise extreme discretion in the type of information posted. In no blog or website, including blogs or sites published from personal or public systems, shall JCU business matters be discussed; confidential, proprietary, or sensitive data be released; or material detrimental to JCU be published. This section is not to be construed as prohibiting either speech

protected by law, including the National Labor Relations Act, or faculty speech protected by Academic Freedom, as described in the Faculty Handbook.

As long as JCU policies, as specified herein, are followed, JCU allows the publishing and use of blogs. However, when done with IT Resources or during business hours, blogging by employees of JCU must either A) be business-related, or B) consume no more than a trivial amount of the User's time and network resources. The User assumes all risks associated with blogging.

T. Messaging. The user should recognize that messaging technologies, such as, and not limited to, email, instant messaging, social media platforms, and SMS (text) messages, unless specific encryption measures are taken, are not considered secure methods of communication. The User must follow all policies to prevent the disclosure of confidential data. Specifically, unencrypted confidential data, such as Credit Card Primary Account (PANs), student data or records, or other Sensitive Data and its supporting standards, must never be sent via messaging technologies in an unencrypted form.

U. Bandwidth Usage. Network bandwidth is a shared resource that must be used as such. Excessive use of JCU bandwidth or other IT Resources, where not required by job function or role as a student, is not permitted. JCU may restrict bandwidth for certain services deemed non-critical to JCU operations, or as it sees fit to preserve network functionality.

V. Social Networking/Social Media. Social networking creates risks for JCU in two ways: 1) in the potential sharing of JCU confidential, private, or embarrassing information, and 2) the potential for an attacker to use posted information to craft a social engineering attack on JCU. The User is asked to recognize that information posted on social networking sites is public information and to exercise discretion in the type of information posted. No confidential or sensitive information belonging or related to the University is to be posted on social networking sites. Further, the user should consider the use of appropriate privacy settings to the fullest extent possible. The University reserves the right to take appropriate action (including but not limited to suspension of access to IT Resources or appropriate corrective or disciplinary actions) related to misuse of Social Networking/Social Media using IT Resources, including when such use is unlawful, poses a safety risk, is offensive, is detrimental to JCU, its students, or employees, or violates the University's mission, vision and values. This section is not to be construed as prohibiting either speech protected by law, including the National Labor Relations Act, or faculty speech protected by Academic Freedom, as described in the Faculty Handbook.

As long as JCU policies, as specified herein, are followed, JCU allows reasonable use of social networking sites from its network and/or during business hours. This use must either A) be business-related, or B) consume no more than a trivial amount of the user's time and IT Resources. The User assumes all risks associated with social networking.

W. Circumvention of Security. Using any computer systems to attempt circumventing any JCU security systems, authentication systems, user-based systems, or the escalation of privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent JCU security systems is expressly prohibited. This includes disabling or tampering with any security software, such as antivirus/anti-malware software or remote access software.

X. Use for Illegal Activities. No IT Resources shall be used for activities that are considered illegal under local, state, federal, or international law.

Y. Overuse and Misuse. Actions detrimental to IT Resources, or that negatively affect student and/or employee job performance, or JCU operations are not permitted. IT Resources should not be used for actions contrary to the University's mission, values, and stated policies. The University reserves the right to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources are used appropriately.

Z. Copyright Infringement. JCU's IT Resources must not be used to download, upload, or otherwise access illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of this Policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using any method, unlicensed websites, or unlicensed media; B) posting or plagiarizing copyrighted material, and/or C) downloading copyrighted files which the User has not already legally procured. This list is not meant to be exhaustive; copyright law applies to a wide variety of works and applies to much more than is listed above. For additional guidance see JCU Copyright Policy and other applicable University policies.

AA. Non-JCU-Owned Equipment.

1. *Non-JCU-Owned Equipment Permitted.* Computer equipment and devices provided by the User or contractor (other than prohibited in section below) are generally permitted to connect to JCU's network and shall adhere to this Policy and all other IT Policies and Standards. Examples of these devices are laptops, notebooks, tablet computers, smartphones, game consoles/devices, etc. Such devices must adhere to the "Sensitive Data" section above, and Policy 100 Cybersecurity Policy.

2. *Non-JCU-Owned Equipment Prohibited.* Non-JCU-provided computer equipment that is prohibited for use at JCU includes any form of network device used for routing traffic such as, but not limited to, hubs, repeaters, gateways, Wi-Fi routers, and firewalls.

BB. Removable Media. In an open environment such as higher education, the use of personal storage devices is common but represents a very serious threat to data security. Examples of these devices are USB drives, flash storage, media players, etc.

When using removable media, all rules for handling confidential data, such as those defined in the Schedule 100 Information Classification Matrix, must be strictly followed. This includes the use of encryption technologies to protect the information stored on these devices in case they are lost, stolen or access is inadvertently obtained. For more information on proper encryption, please visit the ITS website.

CC. Software Installation. Unauthorized installation of non-JCU-supplied software applications on JCU IT Resources is prohibited. Numerous security threats can masquerade as innocuous software. Malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

DD. Reporting of an IT Security Incident. *See something, say something!* It is critical that users immediately report any suspicious activity so the University can quickly mitigate security threats. If an IT security incident or breach of any security policies is discovered or suspected, the User (student, employee, or contractor) must immediately notify the Service Desk. Examples of incidents that require notification include but are not limited to

1. Suspected compromise of login credentials (username, password, etc.)
2. Suspected virus/malware/Trojan infection
3. Loss or theft of any device that contains JCU information
4. Loss or theft of ID badge, keycard, or two-factor authentication token
5. Any attempt by any person to obtain a User's password over the telephone or by email
6. Any other suspicious event that may impact JCU's information security.

EE. Equipment Use and Care. Laptops and other computer equipment and devices must be handled with care, especially during transport. University data-containing equipment may not be baggage checked when traveling. If equipment is packaged for shipping, it must be shipped using a common carrier with tracking and insurance

coverage purchased. Equipment is never to be left unattended, including leaving equipment in plain sight within your vehicle or other mode of transportation.

Equipment may not be altered, disabled, or made to work in a way that is inconsistent with how the equipment was provided. Users must report any lost, stolen, or broken equipment to the ITS Department immediately.

Best practices for equipment use and care also include being sensitive to extreme temperatures when using equipment (the normal operating temperatures for most electronic equipment is 40–90 degrees Fahrenheit), and exercising caution when equipment is close to liquids—generally speaking, electronics and liquids don't mix.

FF. Personal Data on University-owned and Authorized Equipment, The University provides certain employees with laptops, PCs, tablet computers, flash drives, or external hard drives to perform their job functions. Employees who store personal email, pictures, texts, voicemails, etc. on University-owned or University-provided equipment have no expectation of privacy regarding this data.

The University does not assume any responsibility or liability for any loss, disclosure, review, or use of any personal data on a University device. Personal data stored on University-owned equipment and authorized personal devices is subject to deletion by the University if, among other things: the device is lost, stolen, not immediately produced or returned on demand or at the end of employment, or requires reconfiguration, updates, or other work.

GG. Enforcement. Violation of this Policy will result in notification to the appropriate vice president and will be grounds for corrective action under the appropriate University policies. Violations of this Policy may lead to corrective action up to and including dismissal, termination, suspension, termination of access to IT Resources, and/or legal action.

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 (Changes to this definition in POL-100 Sensitive Data and Cybersecurity Policy should be considered authoritative for this policy).

B. **Encryption**: The process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it.

C. **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.

D. **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.

E. **User:** Any individual 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.

F. **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 education records, personal financial records (or other sensitive personally identifiable information), protected 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.

   Examples of Sensitive Data include: JCU ID numbers; protected health information; financial data; educational records; intellectual property records; protected research records; donor profiles; or any information that could result in a material risk of identity theft, a violation of the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the Gramm-Leach-Bliley Act (GLBA), or otherwise 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 (Changes to this definition in POL-100 Sensitive Data and Cybersecurity Policy should be considered authoritative for this policy).

CROSS REFERENCES

University Policies

JCU-IT-POL-100 Sensitive Data and Cybersecurity Policy

JCU-IT-SCH-100 Information Classification Matrix

JCU-IT-POL-106 Identity and Access Management Policy

JCU Copyright Policy

The policy and its accompanying documents are to be reviewed every year. If a policy has expired, the policy shall nonetheless remain in effect until it is updated and approved.