JONES COLLEGE SINCE•1911 | POLICIES

Policy Name:	Electronic Resources Acceptable Use Policy					
Section Number:	4.03	**Section Title:**	Office of the President			
Policy Owner:	Vice President of Information Management		**Last updated:**	February 2020	**Reviewed:**	March 2020
Status:	Active		**Due for Review:**	March 2025		

Jones College supports an extensive information-technology environment for faculty, staff, students, and other members of the College community. The College's general policies and codes of conduct apply to the electronic environment just as they apply in all other College settings. This Acceptable Use Policy (AUP) supplements these existing standards by describing the special rights and responsibilities that attach to use of the College's technology resources (as defined below). This Policy also explains the roles of those charged with maintaining, operating, and overseeing College technology resources.

The entire community's cooperation helps to ensure that high-quality technology resources remain available for the many endeavors of the College and its constituents.

SCOPE

This policy applies to all persons who access or use the College's technology resources (referred to in this policy as "users"), including without limitation the faculty, staff, students, alumni, and guests of Jones College.
This policy applies to all information-technology resources of the College, including without limitation:

- All computers, systems, equipment, software, networks, and computer facilities owned, managed, or maintained by the College for the handling of data, voice, television, telephone, or related signals or information;
- Any access or use of the College's electronic resources from a computer or other system not controlled or maintained by the College; and,
- The creation, processing, communication, distribution, storage, and disposal of information under the College's control.

In addition, members of the Jones College community may have access to third-party electronic resources through their affiliation with the College or of any other contracting party of the College. Use of these resources by members of the Jones College community is governed by this policy and any applicable policy or restriction of the third-party provider.

The staff of the Jones College Information Technology department ("IT staff") is responsible for the administration of this policy.

PURPOSE

The College makes technology resources available to support its academic and administrative goals and uses of technology resources to advance those goals take precedence over all others.

Within the College community, each person will have differing purposes for using and accessing technology resources; however, each person also has a shared responsibility to utilize those resources appropriately and to protect the resources from unauthorized access or use.

Authorized Users

Technology resources must only be used for purposes authorized by the College. These purposes generally comprise work, study, research, service, or student residential activities consistent with the College's mission and priorities.

Jones recognizes that many users participate in outside academic and professional activities that naturally complement the users' on-campus commitments and enhance their contributions to the College. For example, faculty and staff are active in learned societies, professional associations, academic conferences, and the preparation of scholarly publications, occasionally with incidental compensation. Use of technology resources in connection with such activities is generally acceptable as long as the activities are otherwise consistent with Jones's mission and policies. The College also acknowledges that limited personal use of technology resources is compatible with the type of community that the College fosters in support of its broader goals. Such personal use, except by enrolled Jones students, must be incidental at most and may not cause the College to incur additional costs. Above all, use of technology resources for outside or personal purposes is always a privilege, not a right, and may not interfere with use for College purposes.

All use of technology resources must comply with:

- all College policies, procedures, and codes of conduct, including those found in the student, faculty, and employee handbooks;
- all laws and regulations applicable to the user or the College; and,
- all relevant licenses and other contractual commitments of the College, as modified from time to time.

Technology resources may not be used, committed, or made available, without prior authorization of the chief academic officer (in the case of faculty), the chief financial officer (in the case of staff), or the chief student affairs officer (in the case of students), who will consult with the chief information officer, for:

- any ongoing business or other commercial activity not administered by the College;
- the benefit of persons or organizations other than the College.

The College has sole authority to determine what uses of technology resources are proper and may prohibit or discipline use deemed inconsistent with this policy or other applicable standards of conduct.

Email

The College may send official correspondence to members of its community via electronic mail. Students, faculty, and staff are expected to check their @JCJC.edu email account regularly and are responsible for College information sent there. College employees are expected to use their Jones College email account for all College-related communications. If a student elects to forward their @JCJC.edu email to another email account, the student remains responsible for any material not received because of any defect in the forwarding mechanism or the destination account.

Accounts and Access Restrictions

User IDs and passwords are the primary methods used to authenticate users of the College's technology resources. They help prevent unauthorized access to technology resources or any restricted information found within them. Users may not share their passwords with any other person and must protect them from disclosure by, for example, changing them regularly, monitoring access to their accounts, and contacting the College's IT staff if they suspect their passwords have been compromised. Users will be held responsible for all activity conducted using their IDs. Users must select strong passwords (meaning passwords composed of a mix of at least eight numbers, letters, and symbols and not including a word commonly found in a dictionary, or as required by the system at the time of creation). No person, including any member of the IT staff, is authorized to request any user's password.

All users must protect the College's technology resources from unauthorized access. Specifically, all users must:

- Take responsibility for the security and integrity of information stored on any personal or assigned desktop, laptop, or handheld system;
- Take care to access technology resources only from secure environments and to log out of sessions before leaving any computer unattended;
- Take all appropriate precautions when accessing confidential or restricted College data to protect the data from unauthorized disclosures and from threats to its accuracy or integrity;
- Comply with requests from the IT staff and other authorized personnel to cease use of technology resources that compromises the technology resources or the College; and,
- Cooperate with system administrators during investigations of improper use.

And, without authorization, no user may:

- Extend the network by introducing a hub, switch, router, wireless access point, or any other service or device to any College network;
- Provide any other person with technology resources or access to them;
- Send e-mail chain letters or mass mailings for purposes other than authorized College business;
- Alter, remove, or forge email headers, addresses, or messages, or otherwise impersonate or attempt to pass oneself off as another;
- Obtain technology resources beyond those allocated to the user, seek or gain access to data or user accounts for which the user is not authorized, or eavesdrop or intercept transmissions not intended for the user;
- Use the College's Internet or other network access in a malicious manner or to alter or destroy any material which the user is not authorized to alter or destroy;
- Tamper with, modify, damage, alter, or attempt to defeat restrictions or protection placed on accounts or any technology resources; or
- Damage computer or network systems; create or intentionally introduce or propagate computer viruses, worms, Trojan Horses, or other malicious code to any technology resource; attempt to degrade the performance of the system or to deprive authorized users of technology resources or access to technology resources.

Copyright and other Intellectual Property

Users must respect intellectual property rights, including copyrights, in all use of College technology resources. All use of content, including text, images, music, and video, retrieved from technology resources

or stored, transmitted or maintained using technology resources, must comply with copyright and other applicable laws. Copied material, used legally, must be given attribution in conformance with applicable legal and professional standards.

Software may be copied, installed, or used on College technology resources only as permitted by the software's owner or authorized licensor and by law. Proprietary software must be properly licensed, and users must strictly adhere to all applicable license provisions (including those concerning installation, use, copying, and the number of simultaneous users).

Respect for Others

Users must honor the rights of others to privacy, academic freedom, and freedom from harassment. Users may not use technology resources to threaten or harass any person or to create a hostile place to work or study. In particular, users must honor others' requests for the user to stop sending unwanted communications of any kind.

Users may not do anything to interfere inappropriately with others' use of technology resources, including by consuming technology resources in excess.

Users' Expectation of Privacy

The College recognizes the importance of privacy in an academic setting and does not routinely monitor a current user's email, data, software, or other online activity. There are limited circumstances, however, in which the College may access, monitor, limit and/or disclose a user's communications or other data on technology resources without the user's permission. These circumstances include the following:

- To maintain the integrity of its systems, network or data;
- When required by federal, state or local law, administrative rules, court order or other legal authority;
- To preserve the health and safety of individuals or the Jones College community;
- When there are reasonable grounds to believe that a violation of law or a significant breach of College policy may have taken place and access, inspection or monitoring may produce evidence related to the possible misconduct; or
- To address a legitimate business need.

Such College access to a user's communications or other data on technology resources without the user's permission will occur only with the approval of:

- the president
- the chief financial officer (for administrators and staff),
- the chief academic officer (for faculty),
- the chief student affairs officer (for students),
- or their respective designees.

In cases of emergency where necessary to preserve the integrity of the system, comply with laws or other legal authority, or preserve health and safety, the College may access, monitor, limit and/or disclose a user's communications or other data on technology resources without seeking the above-described permission. In that instance, the vice president of information technology or designee will log any emergency access for review by the aforementioned administrators, as applicable.

Finally, the College cannot guarantee the security of those technology resources against unauthorized access or disclosure.

Oversight of Technology resources

Authorized employees of the College, including the IT staff charged with the daily administration of the College's technology resources, may:

- Take all reasonable steps necessary to preserve the availability and integrity of Technology resources, including blocking any user's access to technology resources;
- Reject or destroy email messages, email attachments, and other files suspected of being spam or containing malicious code, such as viruses and worms;
- Exercise administrative authority over networks, systems, or software in order to grant users access to read, write, edit, or delete information in files or databases, to establish security controls and protection for information and technology resources, or to address claims that intellectual-property or other rights have been violated;
- Employ a variety of security monitoring devices and tools to identify misuse or unauthorized use of technology resources;
- With the approval of the Chief Information Officer or the vice-president of Information Technology, temporarily shut off the College's Internet connection, servers, or services, without prior notice, in order to protect College systems, data, and users or to protect other important interests of the College;
- Temporarily or permanently terminate users' use of technology resources to investigate or remedy any threat to technology resources or violation of this policy; and,
- Exercise administrative rights over certain technology resources, if the IT staff delegate those rights.

Disclaimers

The technology resources and anything accessible on or through them are made available "as is" and "as available." The College makes no guarantee that any technology resource will be free of objectionable matter, errors, defects, bugs, viruses, worms, "Trojan horses," or other destructive features. The College is not responsible for any harm arising from technology resources or users' reliance on them, nor is it responsible for any third-party content accessed using College technology resources, including content made available by another College user or any third party.

This policy is not a complete statement of the College's rights or remedies, and nothing in this policy waives any of those rights or remedies, including any rights in or to the technology resources.

Changes to this Policy

The College reserves the right to change this policy at any time. The College will post the most up-to-date version of the policy on the College web site and may, in its discretion, provide users with additional notice of significant changes. A user's continued use of any technology resources after any changes are published binds the user to the revised policy.

SYSTEM ADMINISTRATION SECURITY ACCESS

To Add or Update a User

1. Each department supervisor makes a request for their staff member(s) to be given a log in ID and password to the system. This request is made by the supervisor by calling the IT Helpdesk or by going to the online work order request menu item located through the PeopleSoft link via MyJones. Each request is then handled by the appropriate IT staff.

2. IT creates the user ID, password, and assigns the appropriate menu items as determined by the supervisor.