NICHOLS COLLEGE

Acceptable Use of Information Technology Resources

Purpose

The purpose of this policy is to outline the acceptable uses of computing and information technology resources for the Nichols College community. This policy outlines the standards for acceptable use of college computing and information technology resources that include, but are not limited to, equipment, software, networks, data, and telecommunications services, whether owned, leased, or otherwise provided by Nichols. This policy is intended to reflect the College's commitment to the principles, goals, and ideals described in the Nichols College Mission Statement.

Coordination with Other Policies

Users of information technology resources at Nichols College are advised that other college policies, including those for Human Resources, the faculty and student handbooks, and notably those policies governing copyright and intellectual property compliance, may be related to the use of information technology resources, and that those policies must be observed in conjunction with this policy.

Additionally, laws (including, but not limited to FERPA, HIPAA, etc.) and college policies relating to disclosure of confidential information must be observed.

Access to and Expectations of Persons Using Information Technology Resources

It is the policy of Nichols College to maintain access for its community to local, national and international sources of electronic information in order to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nichols maintains a variety of information technologies for use as resources for people, catalysts for learning, increased access to technology, and an enriched quality of learning. Access to this environment and the college's information technology resources is a privilege and must be treated with high ethical and legal standards.

Both the Nichols community as a whole and each individual user have an obligation to abide by the following standards of acceptable and ethical use:

- Use only those computing and information technology resources and data for which you have authorization and only in the manner and to the extent authorized.
- Use computing and information technology resources only for their intended purpose.

- Protect the access and integrity of computing and information technology resources.
- Abide by applicable laws and college policies and all applicable contracts and licenses; and respect the copyright and intellectual property rights of others, including the legal use of copyrighted material.
- Respect the privacy and personal rights of others.
- Connecting end-user equipment to the network that has appropriately maintained software; including (but not limited to) operating systems, browsers, plug-ins, anti-virus, and other software as appropriate.

Access to Nichols information technology and computing resources is a privilege granted to students, staff, and faculty at Nichols. The college extends access privileges to individual users of the college's information technology and computing resources. The extension of these privileges is predicated on the user's acceptance of and adherence to the corresponding user responsibilities detailed in this policy. The college reserves the rights to limit, restrict, or extend access to information technology resources as it deems appropriate.

Residence Hall Network Access Restrictions

No student shall turn on or connect student owned wireless access points, gateways, or routers in the residence halls or elsewhere on campus. These wireless routers are commonly sold in retail stores and provide home private use; however when brought on campus they cause Nichols College wireless interference, network congestion, and loss of network access to other students.

Application

This policy applies to all users of Nichols computing and information technology resources, including faculty, staff, students, alumni, guests, external individuals or organizations and individuals accessing external network services, such as the Internet via college facilities. The Chief Information Officer will determine operational policies, networking standards and procedures to implement the principles outlined in this policy. The Information Technology department (IT) has the right to protect shared information technology resources.

Ownership

Nichols College assumes and reserves ownership of all data, files, messages, and programs stored in its computer systems and cloud-based services. Users cannot claim ownership of any data stored in Nichols College computer systems. Users can, however, expect exclusive use of all e-mail messages stored in their user accounts. Cooperation with any system administrator requests regarding user computing activities is expected. Only under certain unusual circumstances involving issues of system integrity, sexual harassment, or suspicion of illegal use of computer resources, and at the direction of the president of the college, Chief Information Officer, Vice President for Administration, Director of Human Resources, or Dean of Student Services, will the system administrator access email stored in user accounts.

In the event that any user is separated from the college, for any reason, and their access to technology resources is terminated, the college bears no responsibility to provide the user with copies of any personal data, files, messages, or programs from college resources. The only exception to this policy is for those employees that would like to retrieve academic materials developed and used in support of their teaching and academic leadership responsibilities. In this case, the employee's manager, or their designee, would be responsible for reviewing all files/messages in the applicable folder(s) to ensure that there is no confidential information in the files/messages being copied for the employee.

Copying Copyrighted Materials (software, music, videos)
Respect for the intellectual work and property of others has traditionally been essential to the mission of academic institutions. As members of the academic community, Nichols College values the free exchange of ideas. Just as Nichols College does not tolerate plagiarism, it does not condone the unauthorized copying of any copyrighted materials. The copying of these types of materials without the permission of its owner is illegal and a criminal offense.

Storage/Copying of Confidential and Proprietary Information
Nichols maintains systems that store a significant amount of confidential information on faculty, staff, students, donors, prospects, vendors, etc. Access to this information is restricted based on a need to know. Under no circumstances is confidential information to be copied or exported off the server and stored on a laptop/portable computer, tablet, desktop computer, home computer, cloud-based storage (except for I.T. provisioned storage such as the Office365 suite of storage services), smart phone, or removable storage media, including, but not limited to, CD/DVD, USB key/thumb drive, or IPOD/MP3 players.

With regard to cloud-based storage of files, the College must insure continued access to confidential information in the event that an individual severs ties to the College, whether the separation is amicable or otherwise. Therefore, the only cloud-based storage allowed is that which is provisioned by I.T. staff.

It should also be understood that e-mail messages, which have file attachments containing confidential information, run the same risk of exposure as files on removable storage media, laptops, tablets, or smart phones. Therefore, files containing confidential information must not be attached to any e-mail messages.

The restrictions listed above for confidential information also apply to the storage of College-proprietary information.

Use of College-Assigned Usernames and Passwords
Nichols College assigns usernames and passwords to individuals to provide users with access to specific information and system resources, based on the needs of their job function. Under no circumstances are users to share usernames and passwords with anyone else, unless requested to do so by a system administrator

for the purpose of troubleshooting a system issue. Sharing of this information will be construed as circumventing the college's security practices and procedures, and will expose that user to risk of disciplinary action. Any need for system access to data or resources must be processed as a request through the appropriate channels, so that appropriate authorizations can be obtained and documented.

Right to Monitor and Access

The campus computer systems linked together on a common fiber-optic network are owned by Nichols College, or, in some cases, are privately owned as personal computers brought to campus by faculty, staff, or students. Regardless of ownership, every computer attached to the campus network for any reason (e.g., Internet connectivity, e-mail accessibility, etc.) is subject to monitoring by the IT staff. <u>Devices and information stored on the Nichols College network are not private</u>. Thus, any information users input or transmit on the Nichols College network can and may be reviewed by the college without prior notice to them, even if that information is protected by an individual password. Nichols College explicitly reserves the right to access, monitor, review, copy or delete any information stored or transmitted on any device on the college network at any time as the college deems appropriate. This may include random, unannounced audits to ensure that the college's information systems are being used in accordance with this policy.

Uses

In general, the Nichols College academic community shall use college information technology resources (which include privately-owned computers connected to the college network) in connection with the college's core teaching, research, and service missions. Uses that do not significantly consume resources or interfere with other users also are acceptable, but may be restricted by IT. Under no circumstances shall members of the college community or others use college information technology resources in ways that are illegal, that threaten the College's tax-exempt or other status, or that interfere with reasonable use by other members of the college community. Any use of college information technology resources, including network infrastructure, for commercial purposes is prohibited.

Sanctions for Violations

Failure to comply with the appropriate use of computing and information technology resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the secure environment for creating and maintaining information properly, and subjects one to disciplinary action. Any member of the Nichols community found using computing and information technology resources in violation of this policy is subject to existing disciplinary procedures including, without limitation, suspension of system privileges, expulsion from school, termination of employment and/or legal action as may be appropriate. Nichols College also reserves the right to confiscate any privately-owned equipment that is used in the violation of this Acceptable Use Policy.

Review of the Policy

This policy may be assessed from time to time to reflect substantive change as a result of changes to the Nichols College information technology resources and/or changes in legal statutes that impact information technology resources, copyright, or other intellectual property issues. The Chief Information Officer is responsible for determining when the policy needs to be reviewed and the process for review and revision.