CARLOW UNIVERSITY
Values. Scholarship. Vision.®

Policy #: 02-200
Effective Date: 4/7/2016

Responsible Use of Information Resources

Category: Information Technology

Purpose: The purpose of this policy is to describe what is considered acceptable and unacceptable use of the University's technology infrastructure.

Scope: The University has implemented a technology infrastructure to support its mission. While it may be acceptable to use these resources and services for authorized purposes that do not directly support the University's mission as set forth herein, it is not acceptable to use them for purposes which are in conflict with the mission or are unlawful.

Responsible Party: Senior Technology Officer

Related Policies: Replaces outdated legacy documents 07-000 through 07-700
Related to New policy 07-001, Technology Purchasing

Table of Contents

Timeline/Revision History 2
Details 2
Definitions 2
Access to Services 2
Off-campus access to services 3
Protection of accounts and information 3
Personal devices on Carlow network and use of Information Resources 4
Mobile devices such as smartphones, tablets, laptops 4
Inappropriate behaviors 5
Process for reporting suspected inappropriate behavior 5

Responsible Use of Information Resources

Timeline/Revision History

Origination: March 2015
Technology Advisory Council Review and modifications: March-June 2015
Campus comment: Oct-Nov 2015
Cabinet and President Review: February 2016
Legal review: March 2016
Cabinet and President Consensus: April 2016

Details

In support of its mission, Carlow University, within the parameters of institutional priorities and financial capabilities, provides access for faculty, staff, students, Sisters of Mercy, contractors, and guests (hereinafter "Users") to local, national and international sources of information.

The policy for Responsible Use of Information Resources contains the governing philosophy for regulating any and all use of the University's Information Technology Resources including, but not limited to University-owned and/or licensed computers, software, telephone equipment and services, audio-visual equipment, learning spaces resources, websites, forums, databases, Internet bandwidth, networks and networking equipment. The policy also addresses acceptable use of any personally owned devices, such as tablets, smartphones and laptops connected to, through, or gaining access to networks, databases, or websites administered by the University. In adopting this policy, the University recognizes that all members of the University community are also bound by local, state, and federal laws governing the use of these resources.

Definitions

User: Any person who utilizes University Technology including, but not limited to: students, faculty, staff, Sisters of Mercy, contractors, and guests.

University Technology: The network equipment, internet connections, computers, audio-visual equipment, telephones, and related technical devices that enable the display or sharing of information

Information Resources: University Technology, software applications, information databases and services, data, digital documentation, and user accounts.

Access to Services

Access to the University's Information Resources is a privilege granted to Users. The University reserves the right to extend, limit or revoke privileges and access to these Resources. Any User who, without authorization, overburdens, accesses, destroys, alters, dismantles, or disfigures University Information Resources, properties or facilities, including those owned by third parties, thereby threatens the environment of increased access and sharing of information. This unauthorized use is considered unethical and unacceptable conduct, as it threatens the security and viability of the Information Resources of the University. Whether intended, accidental or

unwittingly engaged in, such behavior is unacceptable and subjects the User to discipline, sanction or report to law enforcement, as applicable.

Carlow University's Technology, including the campus network and access paths it provides to off-campus resources such as the Internet, are facilities of the University and are designed to advance the mission of the University. The University strives to operate its Technology reliably, efficiently, securely, legally, and in accordance with University policies. To accomplish this, the University may exercise its right to log access to and use of all resources on its network as well as the digital traffic that flows through its network.

Although information can be monitored and logged by the network, the University does not routinely monitor individuals' activities or the content of their use of University owned and administered technology resources. The University reserves the right to monitor or review individual activity or content on University-owned or provided services. The University will take all appropriate steps to identify the cause and/or source of any identified problem with the operation of its network or information resources or any violation of its policies. This may include using information logged by the system or collected about users and the devices they use. If policies are violated, offending users will be dealt with according to established procedures. If there are indications of local, state or federal law violations, University personnel will cooperate with law enforcement or other appropriate individuals to identify and prosecute offenders. This will include providing information about machines and user activities that might be involved in the violations.

Certain student information is protected by state and federal regulations, such as FERPA. The ability by employees to access student and employee data is limited and based on the responsibilities of that employee's professional position. It is the responsibility of each employee to act ethically, within the scope of University policies and applicable laws when accessing or utilizing this data. Faculty and staff are also expected to protect the privacy of University information when utilizing any method of storing, sharing, or delivering information, data, and equipment to or from an off-campus location, and to return, restore, or forfeit possession of any requested University materials or resources at the end or termination of an agreement or at the request of the University.

Off-campus access to services

The use of the University Technology for conducting University business is permitted when off-campus. Faculty and staff are able to access secured and protected services, information, data, sites, and equipment.

Faculty and staff are encouraged to exercise additional precautions to protect information when accessing information from remote locations. All policies and expectations contained within this policy are in full force, regardless of geographic location.

Protection of accounts and information

It is the responsibility of each person to set strong passwords and to ensure that their passwords remain private. Sharing of accounts and passwords is a violation of this policy, as it may allow for unauthorized access or damage to the University's technology

Information systems are configured with timed locking mechanisms and password change requirements to protect access to data. However, it is incumbent upon Users who are granted the privilege of accessing sensitive information to take appropriate measures to log-out and secure both digital and physical information.

The University encourages innovative solutions in the use of technology while upholding the need to protect sensitive information. Confidential information, including any data protected by FERPA or other legislation, may be stored in non-University systems (e.g., cloud services) only after formal permission of the senior technology officer and upon satisfactory acknowledgment and legal review of data ownership and security, sharing, backup, and recovery policies of the external device or service.

Personal devices on Carlow network and use of Information Resources

Carlow University provides the privilege of connecting personal devices to the campus network to gain access to internet resources. This may be referred to as "Bring Your Own Device" or (BYOD). As such, Carlow requires that all devices have appropriate and up to date anti-virus software installed. Additionally, Carlow reserves the right to restrict or deny access to any personal device that either does not meet the minimum requirements to protect the security of the network or the services therein, or any device that hampers the effectiveness of the network services. The use of any personal network routing device with the University technology is strictly prohibited. Carlow reserves the right to monitor and verify for connection of devices to the University technology, which, if found, subjects the User to discipline, sanction or report to law enforcement, as applicable.

Mobile devices such as smartphones, tablets, laptops

With the mobility of information available via laptops, tablets, thumb drives, cloud-based storage, CD backups, etc., the University requires that anyone using such devices and/or services take precautions to protect sensitive and confidential information. Confidential information is to be encrypted and/or stored on password-protected devices. Access by any employee to any University operational information, including e-mail services, must be on a device which can be remotely erased in the event of loss, theft, or transfer of custody. By connecting a personal device to any University Technology, the owner grants permission to the University to execute such management capability necessary to protect the privacy of Information Resources, as well as the capability to protect itself from infrastructure threats by means of interacting with or scanning the device using anti-virus software. Any device which connects to the University Technology must also contain locking security such as password protection or activation. If a personal device containing or used to access University data or information is lost, stolen, or becomes inaccessible to its owner, it is the responsibility of the individual who used the device to access University data or information to contact Carlow University's senior technology officer immediately upon loss of custody of the device in order to safeguard any University information stored therein.

Responsible Use of Information Resources

Inappropriate behaviors

1. Use or attempted use, not authorized by the University, of any University account or resource;
2. Disguise or attempted disguise of the identity of an University account or information resource;
3. Authorization of use of your University account or the accounts of others in the absence of the owner of the account;
4. Use of University telecommunications network to gain or attempt to gain unauthorized access to local or remote information resources, including attempted access to other's account or information;
5. No machine configured to operate as a network server shall be connected to the campus network by any method (data jacks, hubs, wireless or other connections or wifi access points) without written approval from the senior technology officer.
6. Installation of software on corporate-owned devices;
7. Acts performed knowingly or deliberately which are intended to or have the effect of impacting adversely the operation of information resources and/or denying service to other users of the resources. This includes, but is not limited to, the unauthorized use of accounts for the purpose of sending e-mail mass mailings or chain lettersor executing programs that impede the operation of the network;
8. Modification of files, disks, programs or other information resources belonging to the University or other persons without the owner's permission;
9. Use or installation of a program or device which is intended to scan or damage an information resource file, system or network;
10. Circumvention or attempts to circumvent information resource protection measures;
11. Violation of licensing agreements for information resources, including the Digital Millenium Copyright Act (DMCA);
12. Unauthorized reading, copying, deleting or altering in any way information resource communications, files, or software belonging to others without their permission. Authorization to access sensitive data may only be authorized if necessary by the President, Presidential designee, or the senior technology officer;
13. Use of University technology and information resources for personal commercial enterprises (such as side businesses and non-profit operations outside the scope of Carlow University) and/or for financial gain.
14. Unapproved sharing of sensitive, confidential or internal business-related information with any outside agency.

Process for reporting suspected inappropriate behavior

Any suspected inappropriate behavior that counters the Responsible Use of Information Resources should be reported immediately to the senior technology officer. The senior technology officer may report the behavior to other appropriate officials for further action. The University will investigate and address as appropriate any suspected inappropriate behavior in accordance with the student code of conduct, faculty handbook, code of ethical conduct, University policies or any applicable local/state and/or federal law.