CENTENARY UNIVERSITY

Office of Information Technology

Network Use Policy

Purpose

This policy seeks to define acceptable use of University network resources and internet access.

Overview

Centenary-owned computer systems are provided and maintained to support the educational and administrative functions of Centenary University. All material within university-owned computers or systems is subject to review.

Any users of the university-owned networks or systems must abide by the following terms of use. When connected to the Centenary network, all BYOD (personally owned) computer systems, handheld devices, gaming systems, or any other technology devices must also adhere to these policies.

Policy

The following practices constitute **improper** use of Centenary University Technology resources:

- Use that impedes or harms others
- Use that harasses or threatens others
- Attempts to disable or circumvent system security or policies
- Unauthorized access or use
- Unauthorized modification or removal of data or equipment
- Use of unauthorized devices
- Disguised use
- Distribution of computer viruses or other harmful programs
- Use in violation of state or federal laws
- Use in violation of any Centenary University policies
- Any other use of IT resources deemed improper by Centenary University

Administration

Precautions will be taken to reduce the exposure of the network, critical systems and data to threats. The Centenary OIT department reserves the right to set the security level that it deems appropriate on University-owned systems. The administration and security level may be further constrained for any computer found to contain unauthorized installs, tampered accounts, viruses, spyware, or other dangerous software.

Use of Internet

Internet access is to be used in a manner that is consistent with the Centenary's standards of conduct. Centenary is not responsible for material viewed or downloaded by users of the Internet. Users are cautioned that many Internet resources include offensive, sexually explicit, and inappropriate material. Users accessing the Internet do so at their own risk.

Users should never:

- Visit Internet sites that contain racist, sexually explicit, hateful, illegal, or otherwise objectionable materials.
- Post offensive material on the Internet including racist, sexually explicit, hateful, sexist, or defamatory comments.
- Transmit software or copyrighted materials belonging to Centenary or third parties, unless permitted under a license agreement.

Authorized Wifi Access

University-Owned Standard Hardware including assets issued to faculty and staff are joined to the CENTU-SECURE wireless network utilizing WPK2 security.

Staff and Faculty can log into the **CENTU-STAFF** wireless network on their **BYOD Devices (**laptops, tablets, and mobile devices) using their Centenary credentials.

Students can log into the **CENTU-STUDENT** wireless network on their **BYOD Devices (**laptops, tablets, and mobile devices) using their Centenary credentials. **Students** can also make use of the **CENTU-MEDIA** wireless network by registering the device details and MAC Address of devices used in the dorms for media streaming, gaming, and entertainment.

Public users and visitors are constrained to the Guest network (**CENTU-GUEST**) for Internet access.

Software Transmission

- Unauthorized transmission of software is strictly prohibited in order to protect Centenary's computer network, systems, and data.
- Only software approved by Centenary OIT may be transmitted or installed on University-owned equipment.
- On University-owned equipment, certain administrative actions will be disabled, including the ability to install or modify software.

Virus Detection and Prevention

- Viruses, spyware and malware can cause substantial damage to computer systems. Each user is responsible for taking precautions to ensure that viruses are not introduced onto the Centenary network.
- All University-owned assets are equipped with virus protection software that is centrally administered. Users of University-owned assets must permit the virus protection software to update and receive new definitions when prompted to ensure optimal protection from threats.
- All material received from any external medium and all material downloaded from the Internet or external computers or networks must be scanned for viruses and other dangerous programs before being placed onto the computer system.
- Any user who suspects virus, spyware, or malware on University-owned computer system must report it to OIT immediately.
- BYOD computers using the Centenary network must have an up-to-date approved antivirus program prior to connecting to the Centenary network.
- Any unverified equipment will be contained to the GUEST network.

Violations

If a violation of this policy occurs, Centenary University may enforce one or more of the following:

- Suspend, limit, or block access to college networks or systems
- Enforce disciplinary action up to and including termination or expulsion
- Refer suspected violators to the appropriate law enforcement agencies

Approval

APPROVED 10/2019 by Executive Staff