Office of Information Technology

Bring Your Own Device (BYOD) Policy

Overview

Bring your own device (BYOD) refers to the practice of using a personal computing device (computer, tablet, phone, etc.) for work or business related activities. Centenary University does not require employees to use personal equipment for business operations. Those employees who wish to use their personal devices must abide by the policy below. Centenary University is not responsible for the purchase or costs associated with use of personally owned devices.

In response to an increase in personally owned devices being used in the work environment, Centenary has established an official Bring Your Own Device (BYOD) policy.

Purpose

This policy defines the appropriate use and procedures for using personally owned computing devices on the Centenary network and the storage of intellectual property, sensitive data or University licensed software.

Scope

This policy applies to employees, faculty, students, guests and any other user that utilizes the network or computing resources provided by the University for business related activities with a personally owned device such as:

- Portable computers; e.g.; laptops, notebooks, netbooks
- Portable storage media; e.g.; USB storage devices, flash memory cards, CD/DVD ROM
- Mobile devices; e.g.; cellular smartphones, tablet computers

In some cases, these restrictions may be lifted by other official policies pertaining to certain staff, systems, or processes.

Policies

Faculty, staff and students who choose to participate in BYOD must abide by this policy and all University policies while using a personally owned device on the Centenary network.

Employees who participate in the BYOD policy must:

- Not store Personally Identifiable Information or Sensitive Information on personally owned devices.
- Not access Personally Identifiable Information or Sensitive Information from personally owned devices; unless explicitly authorized by a member of Executive Staff.
- Destroy, remove or return all data, electronic or otherwise belonging to Centenary, once their relationship with the University ends or once they are no longer the owner or primary user of the device. (e.g. the sale or transfer of the device to another person)
- Notify the Information Technology Department of any theft or loss of the personal device containing data belonging to Centenary University.
- At no time may the personal device be connected to the CENTU-SECURE network.
- Employees are expected to refrain from using their personal computing devices to conduct University-related business communications while operating a vehicle. This prohibition includes using a personal computing device to place or receive calls or voicemail messages, read or respond to e-mails, text messages, or instant messages, surf the Internet, or for any other purpose related to work while operating a vehicle. Employees who are charged with traffic violations resulting from the use of their person computing device while driving will be solely responsible for all liabilities resulting from such actions.

BYOD Device Support

All devices connected to the University network are required to adhere to the Acceptable Use Policy. Devices must be authenticated under the users account and be current on all software updates and anti-virus solutions in order to use the CENTU-STAFF network. The CENTU-GUEST network is available for devices that do not comply with the restrictions.

OIT may, without notification, prevent or ban any personally owned device which disrupts any University Computing resource or are used in a manner which violates any University policy.

Technical support for personally owned computing devices is **limited** to the following:

- Troubleshooting network connection issues while on the campus network.
- Configuration of email clients for connection to the email system.
- Configuration of the SSL VPN client to allow access to secure resources with approval.

Support services that will not be provided, include, but are not limited to:

- Troubleshooting device performance or hardware problems
- Installation of new or replacement hardware
- Troubleshooting software applications or cloud services
- Installing operating system updates, patches or software applications not required for job functions
- Backing up device data or migration to another device
- Third party email clients/accounts
- Removal of malware, spyware or virus

CENTENARY UNIVERSITY

Office of Information Technology

User Responsibilities

As a user of Information Technology resources you have the following responsibilities:

- You are responsible for registering your network devices in the network registration database in order to maintain access to the network.
- You are responsible for all traffic originating from your networked devices whether you generate the traffic, or not.
- You are responsible for abiding by all applicable laws set forth by Federal, State and Local Governments.
- You are responsible for protecting your privacy.
- You are responsible for not violating the privacy of others.
- You are responsible for keeping your network devices up to date with current security patches.
- You are responsible for using anti-virus software and ensuring that such software is at the most current release.
- You are responsible for protecting any and all sensitive data for which you have access to.
- You are responsible for following all applicable university policies relating to your use of Information Technology resources.
- You are responsible for ensuring the security of Information Technology resources under your direct control.
- You are responsible for securing your granted access privileges and passwords for Information Technology resources.

Risk, Liabilities and Disclaimers

Employees who elect to participate in BYOD accept the following risks, liabilities and disclaimers:

- At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device; nor personal data. It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems before requesting assistance from OIT.
- OIT provides limited security for the wireless networks and at no time does the University accept liability for the security of the personal device when accessing the wireless networks.
- If determined that the use of the personal device is not required for job functions, the University may elect to discontinue providing computing resources to the device.
- The personally owned computing device is subject to the search and review as a result of litigation that involves the University.

- No employee or student should expect a guarantee of privacy in communications over the Internet and University network.
- Violations of this Policy may be discovered by routine maintenance and monitoring of electronic communication systems and network, any method stated in this BYOD Policy, or pursuant to any legal means. The employee and student consents to monitoring, accessing, investigating, preserving, using and/or disclosing any electronic communications that utilize the University's networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to the extent permitted by law.
- Centenary reserves the right to review, retain or release personal and Centenary-related data on personal computing device to government agencies or third parties during an investigation or litigation.

Reimbursement

Computer technology purchased for personal use will not be reimbursed by the University.

This includes all hardware, software, licenses, and technology services, including repair or technical support services purchased with personal funds, regardless of intended use.

Enforcement

Employees and other persons employed by the university found to have violated this policy will be subject to disciplinary action based on the nature of the offense up to and including termination of employment.

Students and guests that are found to have violated this policy will be subject to disciplinary action based on the nature of the offence including but not limited to loss of network and computing access, and other actions the university administration deems appropriate.

Approval

APPROVED 10/2019 by Executive Staff