Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Personally-Owned Device Usage Policy

PURPOSE:

This policy applies to any hardware and related software that is not owned or supplied by Clarendon College, but could be used to access Clarendon College resources. This applies to all Clarendon College agents who have personally acquired a device but also wish to use this device in the business environment.

SCOPE:
All users employing a personally-owned device connected to the Clarendon College network, and/or capable of backing up, storing, or otherwise accessing college data of any type, must adhere to college defined policies, standards, and processes.

PRIVACY:
All users of College networks and systems should keep in mind that all usage of information technology resources can be recorded and is the property of Clarendon College. Such information is subject to the Texas Public Information Act and the laws applicable to college records retention. Employees have no right to privacy with regard to use of college-owned resources. Clarendon College management has the ability and right to view employees' usage patterns and take action to assure that College resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on Clarendon College information technology resources that are owned, leased, administered, or otherwise under the custody and control of Clarendon College are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 1 TAC§202 (Information Security Standards).

GUIDELINES FOR ACQUISITION AND USE:
Employees and other agents must appropriately secure the device to prevent data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse to the college's computing infrastructure by following security guidelines.

a. Employ some sort of device access protection such as, but not limited to, strong passcode, facial recognition, card swipe, fingerprint, etc.

b. Set an idle timeout that will automatically lock the device if misplaced

c. Keep the device's software (operating, anti-virus, security, encryption, etc.) up-to-date

d. Enroll your device in “Find my phone” or similar services and/or label your device with some identifying information (work or home phone number, name, and or address) to make the device easy to return if lost or stolen, this may be done via your locked screen.

e. Report immediately to your manager any incident or suspected incidents of unauthorized data access, data or device loss, and/or disclosure of system or participant organization resources as it relates to personally-owned devices. (Managers will immediately report such incidents to the Clarendon College Vice President of Information Technology).

Sensitive and private data must not be stored on these devices or on external cloud-based personal accounts, such as Office365, Dropbox, or Box.net.

At the time that use of the personally owned device for college business is no longer required the employee will provide documentation to their manager acknowledging and confirming that the device does not contain any Clarendon College sensitive data.

Employees and other agents must:

a. Complete the Cyber Security Training

b. Sign and return the Clarendon College Non-Disclosure Agreement.

ADDITIONAL CONSIDERATIONS:

Employees using prior approved personally owned devices may not be reimbursed by the college for purchase or for monthly service expenses unless so authorized by the college president.

Loss, theft, or damage to personally owned devices will not be reimbursed by the college. This includes, but is not limited to, when the device is being used for college business, on college time, or during business travel.

Personally Owned devices used to access, store, back up, or relocate any college or client specific data may be subject to the search and review as a result of litigation that involves the college and in accordance with the State of Texas Open Records Act.

Clarendon College reserves the right to implement technology to enable the removal of college owned data and to monitor access in order to identify unusual usage patterns or other suspicious activity. This monitoring may be necessary in order to identify accounts/computers that may have been compromised by external parties.

Failure to comply with the Clarendon College's Personally Owned Device Usage policy may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.

DEFINITIONS:

Bring Your Own Device (BYOD): Refers to employees taking their own personal device to work, whether laptop, smartphone, or tablet, in order to interface with the internal/participant organization's network resources. This also refers to mobile storage devices such as USB drives, external hard drives, etc.

Confidential Data: Data for which restrictions on the accessibility and dissemination of information are in effect. This includes information whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act (HIPPA), PCI standards, as well as, data not releasable under the Texas Open Records Act, the Texas Open Meetings Act, or some other statute.

Public Data: Data elements that have no access restrictions and are available to the general public. This data can also be designated as unrestricted data.

Prior Approval: A process by which all users must gain approval prior to working with, utilizing, or implementing a process or procedure.

Sensitive Data: Data for which users must obtain specific authorization to access, since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the participant organization. Example: personally identifiable information (PII), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA) PCI standards, as well as, data not releasable under the Texas Open Records Act, the Texas Open Meetings Act, or some other statute.

Use: Use includes accessing, inputting, processing, storing, backing up, or relocating any Clarendon College or client specific data, as well as, connecting to a network.

Devices: Devices include smartphones, tablets, laptops, desktops and mobile storage devices such as USB drives, external hard drives, etc.

Agents: Agents include employees, including full- and part-time staff, students, consultants, and other agents.

RELATED POLICIES, REFERENCES AND ATTACHMENTS:
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology.
Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website. Also, please see the following related policies below;

a. Clarendon College's Acceptable Use Policy
b. Clarendon College's Authorized Software Policy

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.