Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Portable Computing Policy:

PURPOSE:
Clarendon College may, at its discretion, provide portable computing devices and media to employees. The portability offered by these devices and media increases the risk of unauthorized disclosure of stored information.

To maintain the confidentiality, integrity, and availability of data and network resources at Clarendon College, the Portable Computing Policy establishes requirements for safeguarding electronic devices that can contain protected data.

SCOPE:
The Clarendon College Portable Computing Policy applies to all individuals who use portable computing devices and media, whether Clarendon College-issued or privately owned, to access the Clarendon College information technology computing environment.

POLICY STATEMENT:
Clarendon College's policy is to protect mobile computing devices and the information on such devices. Individuals who use these devices must protect the hardware provided from theft and unnecessary damage and the data stored on them.

As a general practice, sensitive information should only be stored on servers. Data owners must carefully evaluate the risk of lost or stolen data against efficiencies related to mobile computing before approving the storage of confidential or sensitive information on portable computing devices.

The users of portable computing devices or media used to store, transmit, or process protected data are expected to take all appropriate measures and precautions to prevent the loss, theft, damage, and/or unauthorized use and shall include the following:

1. Physically and logically safeguard the devices.
2. Ensure that College-approved anti-malicious software applications and signatures are up-to-date.
3. Use encryption to safeguard all storage media (e.g., hard drives, USBs).
4. Avoid unsecured or untrusted networks.
5. Confidential information should not be accessed over unsecured or untrusted networks.
6. Confidential information should not be stored on a portable computing device.
7. Installing mobile device security software on all college mobile computing systems to secure and track all mobile computing devices, i.e., tablets and laptops.
8. Prevent the use of the portable computing device or media by unauthorized persons;

are responsible for any misuse of the information by persons to whom they have given access.

9. All reasonable precautions to prevent data compromise should be taken when using portable computing devices (e.g., shield screen from passive viewing, password-protected screen saver).
10. Keep portable computing devices within view or securely stored.
11. Ensure the device is shut down or secured when not used (e.g., password-protected devices offering such capabilities).
12. Unattended portable computing devices must be physically secure (e.g., locked in an office, desk drawer, or filing cabinet; in an automobile, safe in a non-visible location).
13. Promptly notify Clarendon College-IT if any portable computing device or media has been lost or stolen.

Requests for exceptions to this policy must be submitted in writing and will be reviewed on a case-by-case basis, see Compliance Policy and Policy Exemption Form. To address a specific circumstance or business need, the Vice President of Information Technology may grant an exception to the encryption requirement for portable devices.

DEFINITIONS:
Encryption: At its most basic level, encryption protects information or data using mathematical models so that only the parties with the key to unscramble it can access it.

Malicious Software: A term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

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.
The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.