Clarendon College
System Information Technology Services CLARENDON COLLEGE-IT)
Authorized Software Policy:

PURPOSE:
Authorized software is any software that is acceptable for use on Clarendon College information technology resources. The Authorized Software Policy aims to provide measures to mitigate information security risks associated with authorized software.

Clarendon College has negotiated special pricing and licensing for software available to all students, faculty, and staff. Other software is readily available in the open marketplace with some licensing agreement under which the user is subject. Some software is considered to pose a security threat to Clarendon College, and its use may be restricted.

Users entrusted with Clarendon College information technology resources are responsible for maintaining licensing information for any software the user installs and, if requested by the College, must provide Clarendon College with licensing information. This includes, but is not limited to, smartphones, iPads, tablets, laptops, etc.

Non-compliance with copyright laws regarding software is subject to civil and criminal penalties imposed by federal and state laws. These penalties apply to the College and/or an individual.

SCOPE:
The Authorized Software Policy applies to all Clarendon College information technology resource users.

POLICY STATEMENT:
All software installed or used on College-owned information technology resources must be appropriately licensed.

Clarendon College-IT shall maintain sufficient documentation to validate that the software is appropriately licensed. Persons installing or authorizing software installation should be familiar with the terms of the agreement.

Users shall accept the responsibility to prevent illegal software usage and abide by College policy on using copyrighted materials, requiring the College community to respect copyright law. These responsibilities include:

1. Do not illegally distribute or share software with anyone.
2. All software must be license-compliant, including personally purchased software.
3. All software licenses must be readily available.
4. Report any suspected or known misuse of software to Clarendon College-IT.

The following general categories of software are prohibited explicitly on all Clarendon College Information Technology Resources unless specifically authorized by the Information Security Officer:

1. Software used to compromise the security or integrity of computer networks and security controls, such as hacking tools, password descramblers, network sniffers, and port scanners.
2. Software that proxies the authority of one user for another to gain access to systems, applications, or data illegally.
3. Software instructs or enables users to bypass normal security controls.
4. Software that instructs or enables the user to participate in any activity considered a threat to local, state, or national security, including the assistance or transfer of information leading to terrorist activity or construction or possession of illegal weapons.
5. Any other software prohibited explicitly by the Information Security Officer.

DEFINITIONS:
Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

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.