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 purpose of the Authorized Software Policy is to provide a set of measures that will mitigate information security risks associated with authorized software.

Clarendon College has negotiated special pricing and licensing for a variety of software available to all students, faculty and staff. Other software is readily available in the open market place that has some kind of 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, smart phones, 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 are applicable to the College and/or an individual.

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

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 the installation of software 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 the use of 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 specifically prohibited 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, for the purpose of gaining access to systems, applications, or data illegally.
3. Software which instructs or enables the user to bypass normal security controls.
4. Software which 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 specifically prohibited by the Information Security Officer.

DEFINITIONS:
Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department that has the responsibility for maintenance and supervision of 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.
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.

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.