**Clarendon College**
**Information Technology Services (CLARENDON COLLEGE-IT)**
**Acceptable Use Policy:**

**PURPOSE:**

The computing resources at Clarendon College support the educational, instructional, research, and administrative activities of the College and the use of these resources is a privilege that is extended to members of the Clarendon College community. Users of these services and facilities have access to valuable College resources, to sensitive data, and to internal and external networks. Consequently, it is important to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the College will take disciplinary action, up to and including suspension or termination of employment. Individuals are also subject to federal, state and local laws governing interactions that occur on Clarendon College information technology resources.

This document establishes specific requirements for the use of all computing and network resources at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202) and Texas Higher Education Coordinating Board)

**SCOPE:**

The Clarendon College Acceptable Use policy applies equally to all individuals utilizing Clarendon College information technology resources (e.g., employees, faculty, students, retirees, agents, consultants, contractors, volunteers, vendors, temps, etc.).

Information technology resources include all College owned, licensed, or managed hardware and software, and use of the College network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

**RIGHTS AND RESPONSIBILITIES:**

As members of the College community, users are provided with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. There is a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether the user is a College employee or a registered student), and of protection from abuse and intrusion by others sharing these resources.

In turn, users are responsible for knowing the regulations and policies of the College that apply to appropriate use of the College's technologies and resources. Users are responsible for exercising good judgment in the use of the College's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

Users are representatives of the Clarendon College community, and are expected to respect the College's good name in electronic dealings with those outside the College.

**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).

**ACCEPTABLE USE:**

The Clarendon College network exists to support research, education, and administrative activities by providing access to computing resources and the opportunity for collaborative work. Primary use of the Clarendon College network must be consistent with this purpose.

Access to the Clarendon College network from any device must adhere to all the same policies that apply to use from within Clarendon College facilities.

1. Users may use only Clarendon College information technology resources for which they are authorized.
2. Users are individually responsible for appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware, and are accountable to the College for all use of such resources.
3. Authorized users of Clarendon College resources may not enable unauthorized users to access the network. The College is bound by its contractual and license agreements respecting certain third-party resources; users must comply with all such agreements when using Clarendon College information technology resources.
4. Users should secure resources against unauthorized use or access to include Clarendon College accounts, passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
5. Users must report shareware or freeware before installing it on Clarendon College-owned equipment unless it is on the approved software list. A request to install software must be reported to the Clarendon College-IT via email before the installing any software.
6. Users must not attempt to access Clarendon College information technology resources without appropriate authorization by the system owner or administrator.

**RESTRICTIONS:**
All individuals are accountable for their actions relating to Clarendon College information technology resources. Direct violations include the following:

1. Interfering or altering the integrity of Clarendon College information technology resources by:
    a. Impersonating other individuals in communication;
    b. Attempting to capture or crack passwords or encryption;
    c. Unauthorized access, destruction or alteration of data or programs belonging to other users;
    d. Excessive use for personal purposes, meaning use that exceeds incidental use as determined by supervisor; or,
    e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.
2. Allowing family members or other non-authorized persons to access Clarendon College information technology resources.
3. Using the Clarendon College information technology resources for private financial gain or personal benefit. Users are not permitted to run a private business on any Clarendon College information technology resources. Commercial activity is permitted but only for business done on behalf of Clarendon College or its organizations.
4. Activities that would jeopardize the College's tax-exempt status.
5. Using Clarendon College information technology resources for political gain.
6. Using Clarendon College information technology resources to threaten or harass others in violation of College policies.
7. Intentionally accessing, creating, storing or transmitting material which Clarendon College may deem to be offensive, indecent or obscene (other than in the course of academic research or authorized administrative duties where this aspect of the research or work has the explicit approval of the Clarendon College official processes for dealing with academic ethical issues).
8. Not reporting any weaknesses in Clarendon College information technology resources security or any incidents of possible misuse or violation of this agreement by contacting the Information Security Officer.
9. Attempting to access any data or programs contained on Clarendon College information technology resources for which authorization has not been given.
10. Making unauthorized copies of copyrighted or licensed material.
11. Intentionally using or attempting to introduce worms, viruses, Trojan horses or other malicious code onto a Clarendon College information resource.
12. Degrading the performance of Clarendon College information technology services; depriving an authorized Clarendon College user access to a Clarendon College information technology resource; obtaining extra information technology resources beyond those allocated; or circumventing Clarendon College security measures.
13. Downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Clarendon College users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Clarendon College information technology services.

14. Engaging in acts against the aims and purposes of Clarendon College as specified in its governing documents or in rules, regulations, and procedures as adopted by Clarendon College and the Texas State College System.
15. Allowing another person, either through one's personal computer account, or by other means, to accomplish any of the above.

**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.

**Computer Virus:** A type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them.

**Copyright Laws:** A form of protection provided by the laws of the United States to authors of "original works of authorship". This includes literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations.

**Freeware:** Software that is available for use at no monetary cost.

**Information Security Officer (ISO)**: Officer designated to administer the College Information Security Program. Usually this may be the Vice President of Information Technology.

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

**Shareware:** A type of proprietary software which is initially provided free of charge to users, who are allowed and encouraged to make and share copies of the program.

**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.