Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Electronic Communication Policy:

INTRODUCTION:
Clarendon College encourages the use of electronic communications to share information and knowledge, supporting the college's mission of education and facilitating its business operations. To this end, the college supports and provides interactive electronic communications resources and facilities for telecommunications, mail, publishing, and broadcasting. Recognizing the convergence of technologies based on voice, video, and data networks, this Policy establishes an overall policy framework for electronic communications.

PURPOSE:
Electronic communication transfers text, HTML, images, or data through a computer, cell phone, tablet, PDA, or any other communication device. This includes email, instant messaging, texting, web pages, social media, digital signage, blogs, and forums.

Clarendon College's electronic communication services support educational and administrative activities, serving as a means of official communication between users and the college. This policy aims to ensure that these critical services remain available and reliable, and are used for purposes consistent with the College's mission.

This policy aims to establish prudent and acceptable practices regarding electronic communication and to educate individuals who use it about their responsibilities associated with such use.

SCOPE:
This policy applies to all members of the Clarendon College community who are entitled to receive electronic communications, including those who send, receive, or store electronic messages.

POLICY STATEMENT:
Under the provisions of the Information Resources Management Act (Texas Government Code, Title 10, Subtitle B, Chapter 2054), information technology resources are considered strategic assets of the State of Texas, which must be managed as valuable state resources.

Clarendon College offers electronic communication services to faculty, staff, students, and other affiliated individuals, including retirees and official visitors. The use of Clarendon College's electronic communication services must be consistent with Clarendon College's educational goals and comply with local, state, and federal laws and College policies.

Communications via Clarendon College's electronic systems are the property of Clarendon College, and management reserves the right to access them when necessary. All user activity on Clarendon College's information technology resources is subject to logging, review, and the

opening of records.

All electronic communication activities must comply with the Clarendon College Acceptable Use and Digital Encryption policies.

All members of the Clarendon College community are responsible for actively monitoring their voicemail, email, and Microsoft Teams messages during school work days. Faculty, staff, and students are required to check their official email addresses frequently and consistently to stay informed about College communications. The College recommends checking email at least once a day, recognizing that certain communications may be time-critical. (Also referenced in the Clarendon College Email Usage Policy.)

The following activities are prohibited as specified by the Texas Department of Information Resources in response to TAC §202 requirements:

1. Sending electronic communication that is intimidating or harassing.
2. Using electronic communication to transmit or receive material that may be offensive, indecent, or obscene.
3. Using electronic communication for conducting personal business.
4. Using electronic communication for purposes of political lobbying or campaigning.
5. Violating copyright laws by inappropriately distributing protected works.
6. Posing as anyone other than oneself when sending electronic communication, except when authorized to send messages for another when serving in an administrative support role.
7. Sending or forwarding chain letters.
8. Send unsolicited messages to large groups except as required to conduct college business.
9. Sending messages with huge attachments.
10. Sending or forwarding electronic communication likely to contain computer viruses, malware, spyware, or other malicious software.
11. Transmitting electronic messages, material, or emails containing sensitive college or personal data insecurely over an external network. (All sensitive material **must** be securely transmitted or encrypted during transmission; see Digital Encryption Policy.)
12. Electronic communication users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Clarendon College or any unit of Clarendon College unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing Clarendon College. An

example of a simple disclaimer is: "The opinions expressed are my own and not necessarily those of my employer."

DEFINITIONS:

Computer Virus: A type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its 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.

Disclaimer: A statement that something isn't authentic or that someone isn't responsible. For example, "the opinions expressed are my own, not necessarily those of my employer."

Encryption: Converting information or data into a code to prevent unauthorized access.

Electronic Communication: Electronic communication transfers text, HTML, images, or data through a computer, cell phone, tablet, PDA, or other communication device. This includes email, instant messaging, texting, web pages, social media, digital signage, blogs, and forums.

Malicious Software: Malicious software, commonly referred to as malware, is a type of software that harms a computer system.

Malware: Any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Sensitive Data: Information that is protected against unwarranted disclosure. Access to sensitive information should be safeguarded.

Social Media: Computer-mediated technologies that facilitate the creation and sharing of information, ideas, career interests, and other forms of expression via virtual communities and networks.

Spyware: Software that aims to gather information about a person or organization without their knowledge, may send such information to another entity without the consumer's consent, or asserts control over a device without the PC user's knowledge.

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.