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

Clarendon College encourages the use of electronic communications to share information and knowledge in support of the college's mission of education and to conduct the college's business. 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 is the transfer of text, html, images, or data through a computer, cell phone, tablet, PDA or any other communication device. This includes E-mail, instant messaging, texting, web pages, social media, digital signage, blogs and forums.

Clarendon College electronic communication services support the educational and administrative activities of the College and serve as a means of official communication by and between users and Clarendon College. The purpose of this policy is to ensure that these critical services remain available and reliable, and are used for purposes appropriate to the College's mission.

This policy is recognized to establish prudent and acceptable practices regarding the use of electronic communication; and to educate individuals using electronic communication with respect to their responsibilities associated with such use.

SCOPE:
This policy applies to all members of the Clarendon College community who are entitled to electronic communications for the purpose of sending, receiving, or storing of 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 strategic assets of the State of Texas that must be managed as valuable state resources.

Clarendon College provides electronic communication services to faculty, staff and students, and to other affiliated classes of individuals, including retirees and official visitors. Use of Clarendon College 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 electronic systems are the property of Clarendon College, and management maintains the right to access when necessary. All user activity on Clarendon College information technology resource assets is subject to logging, review and open records.

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

All members of the Clarendon College community are responsible for monitoring their voicemail, email, and Teams messages, during school work days at least every 4 hours. During off days or holidays at least once daily.

The following activities are prohibited as specified by 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. Sending unsolicited messages to large groups except as required to conduct College business.
9. Sending messages with excessively large attachments.
10. Sending or forwarding electronic communication that is 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 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.

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

Encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

Electronic Communication: Electronic communication is the transfer of text, html, images, or data through a computer, cell phone, tablet, PDA or any other communication device. This includes E-mail, instant messaging, texting, web pages, social media, digital signage, blogs and forums.

Malicious Software: Malicious software, commonly known as malware, is any software that brings harm to 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, that may send such information to another entity without the consumer's consent, or that 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.
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.