Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Email Usage Policy:

PURPOSE:
To prevent tarnishing the public image of Clarendon College and provide a safe and secure communication system. When an email goes out from Clarendon College, the general public may view that message as an official statement from Clarendon College.

This policy covers the appropriate use of any email sent from a Clarendon College email address and applies to all employees, students, vendors, and agents operating on behalf of Clarendon College.

This document establishes specific requirements for using 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 college community members, users are provided with scholarly and/or work-related tools, including access to the library, specific computer systems, servers, software, databases, campus telephone and voice mail systems, and the Internet. There is a reasonable expectation of unobstructed use of these tools, certain degrees of privacy (which may vary depending on whether the user is a College employee or a registered student), and 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 the appropriate use of the College's technologies and resources. Users are responsible for exercising good judgment when using the college's technological and information resources. Just because an action is technically possible does not mean it is appropriate to perform it.

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.

1. **Responsibility of the Sender:**
    a. Ensure that emails are sent to the correct recipients.

b. Clearly state the purpose of the email in the subject line.
c. Provide all necessary information and attachments.
d. Follow up on essential emails if no response is received within a reasonable timeframe.

2. **Responsibility of the Recipient:**
    a. Regularly check and read emails.
    b. Respond to emails promptly.
    c. Notify the sender if an email has been received in error.
    d. Ensure that email notifications are enabled and functioning.
3. **Accountability:**
    a. The sender is not responsible for any consequences arising from the recipient's failure to check or respond to their email.
    b. The recipient is accountable for staying informed about communications sent to their email address.

PRIVACY:
All users of College networks and systems should remember 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 concerning the use of college-owned resources. Clarendon College management has the ability and right to view employees' usage patterns and act to ensure that College resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on Clarendon College information technology resources owned, leased, administered, or otherwise under the custody and control of Clarendon College are not private. They may be accessed by appropriate personnel following the provisions and safeguards provided in the Texas Administrative Code 1 TAC§202 (Information Security Standards).

ACCEPTABLE USE:
The Clarendon College network supports research, education, and administrative activities by providing access to computing resources and collaborative work opportunities. 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. All employees will receive an email account.
2. Users may use only Clarendon College information technology resources for which they are authorized.
3. Users are individually responsible for appropriately using all resources, including the computer, the network address or port, software, and hardware. They are accountable to the College for all use of such resources.
4. 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 specific third-party resources; users must comply with all such agreements when using Clarendon College information technology resources.

5. Users should secure resources against unauthorized use or access, including Clarendon College accounts, passwords, Personal Identification Numbers (PINs), Security Tokens (i.e., smartcards), or similar information or devices used for identification and authorization purposes.
6. 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 installing any software.
7. Users must not attempt to access Clarendon College information technology resources without appropriate authorization by the system owner or administrator.
8. Email is an official means of communication within Clarendon College. Therefore, the College has the right to send communications to faculty, staff, and students via email and the right to expect that those communications will be received and read in a timely fashion. If you have an Internet Service Provider, you can access the College's email system from on-campus and off-campus.
9. Faculty, staff, and students must check their official email addresses frequently and consistently to stay current with College communications. The College recommends checking email at least once a day in recognition that certain communications may be time-critical.
10. An email account will be removed upon notice of termination from Human Resources unless the Benefits & Payroll Coordinator requests an extension. An extension can either be 30 days, in cases where departments need the ability to transfer information, or on further notice if the person involved will have an ongoing relationship with Clarendon College.
11. Adhere to the Clarendon College Communications Policy.

RESTRICTIONS:

All individuals are accountable for their actions relating to Clarendon College's 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 unauthorized persons to access Clarendon College's information technology resources.
3. Sending Personally Identifiable Information (PII) via an unencrypted or unsecured email is forbidden. The use of secure/encrypting processes is a must when sending any email that contains PII information.
4. Using the Clarendon College information technology resources for private financial gain or personal benefit. Users cannot run private businesses on Clarendon College's information technology resources. Commercial activity is permitted but only for business done on behalf of Clarendon College or its organizations.
5. Activities that would jeopardize the College's tax-exempt status.
6. Using Clarendon College information technology resources for political gain.
7. Using Clarendon College information technology resources to threaten or harass others violating College policies.
8. Intentionally accessing, creating, storing, or transmitting material that 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 study or work has the explicit approval of the Clarendon College official processes for dealing with academic ethical issues).
9. 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.
10. Attempting to access any data or programs on Clarendon College information technology resources for which authorization has not been given.
11. Redirection or automatic email forwarding of the college's email system to a personal email system by college employees is forbidden.
12. Making unauthorized copies of copyrighted or licensed material.
13. Intentionally using or attempting to introduce worms, viruses, Trojan horses, or other malicious code onto a Clarendon College information resource.
14. 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.
15. 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, port scanners, or any other non-approved programs on Clarendon College information technology services.
16. Engaging in acts against the aims and purposes of Clarendon College as specified in its governing documents or rules, regulations, and procedures adopted by Clarendon College, Texas Department of Information Resources (TAC 202), and the Texas Higher Education Coordination Board.
17. Allowing another person, either through one's computer account or 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 is responsible for maintaining and supervising the Clarendon College IT infrastructure.

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.

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

Information Security Officer (ISO): Officer designated to administer the College Information Security Program.

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

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

Encrypted Email: This message has been scrambled to prevent unauthorized access. It's a security measure that protects sensitive information from being read by cybercriminals.

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 17, 2025.