Acceptable Use Policy for Students

Purpose

The purpose of this policy is to outline the acceptable use of technology and systems at Endicott College (Endicott). This policy serves to protect both the students and Endicott by helping to ensure the protection of information systems, including the confidentiality, integrity, and availability of Endicott data.

Scope

This policy applies to all Endicott students that have a legitimate need to access information systems or resources owned or operated by Endicott College.

Policy

Acceptable Use

All Endicott College systems and resources are provided to assist enrolled students with their studies and coursework as well as engage in personal activity. Examples of acceptable use cases include, but are not limited to:

- The use of Endicott College information systems for communicating with faculty and staff. (sending emails for example)
- The use of Endicott College systems and resources to access the internet, watch a video, play games or communicate for personal reasons..
- The Use of Endicott College systems and resources to take a test or do homework.

Unacceptable Use

Unacceptable use consists of any inappropriate and/or unnecessary use of Endicott College systems and data. All Endicott College students should use their best judgment in determining whether a use-case is inappropriate or illegal. If there is any uncertainty as to whether or not the usage violates this policy please contact support@endicott.edu. Examples of unacceptable use include, but are not limited to:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Use of devices with no identifiable owner.
- Use of unapproved devices or media.
- Use of unapproved file transfer methods.
- Unauthorized use or sharing of Endicott College systems, assets, and data.
- Use of personal email where Endicott College email should be utilized.
- Using credentials that are not your own to access Endicott systems or resources or attempting to do so (impersonating another person).
- Bypassing or disabling College security controls.
- Violating established policy, procedure, or processes related to information security and/or cybersecurity.
- Installation of unapproved software on Endicott College systems.

Privileged User Access

Some students may be given enhanced user access to perform certain work. These privileges or accounts are only to be used for their intended purpose.

Security Incident Reporting

Security is a shared responsibility of all Endicott College students. If any Endicott College student has been potentially involved in, observed, or otherwise has knowledge of a security incident (e.g. opening an unknown email attachment, downloading an unknown file, clicking on a suspicious link, seeing Endicott owned technology stolen, etc.) they are responsible for promptly reporting the theft, loss, or unauthorized access.

Policy Compliance

Endicott College reserves the right to audit College networks, systems, workstations, devices, etc.,on a periodic basis to ensure compliance with this policy.

Exceptions

Any exceptions to this policy must be requested and approved in writing. An exception request should be submitted by the student to Information Technology for review and approval by Information Security.

Disciplinary Action

Any students who fail to comply with this acceptable use policy or any other information security policies and procedures will be subject to disciplinary action.