INFORMATION TECHNOLOGY ACCEPTABLE USE #9300

POLICY

Purpose

Ocean County College (OCC) provides a robust information technology infrastructure to support its academic, administrative, and operational mission. This infrastructure includes network access, internet connectivity, and information processing systems for students, faculty, and staff. To ensure the integrity, security, and optimal performance of these systems, OCC enforces principles of acceptable use through this policy.

Scope

This policy applies to:

- All OCC-owned, managed, or processed systems and information.
- All authorized OCC personnel and users.
- Any external or non-OCC systems that interconnect with or exchange data with OCC systems.
- All devices used to access OCC systems, including OCC-issued equipment, personal computers, mobile devices, and other electronic devices.

Compliance Requirements

OCC is required to comply with the Gramm-Leach-Bliley Act (GLBA), which mandates adherence to the security standards outlined in NIST Special Publication 800-171, Revision 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

Acceptable Use Guidelines

Users are granted access to OCC's information systems and resources solely to perform their academic or job-related responsibilities. Personal use is not permitted. All users must:

- Use OCC systems in a manner that protects the confidentiality, integrity, and availability of information assets.
- Comply with all applicable federal, state, and local laws, as well as OCC policies and standards.
- Understand that access and use of OCC systems is a revocable privilege and employees and students may be subject to disciplinary action for inappropriate use of OCC systems.
- Be accountable for all activities conducted under their OCC accounts, regardless of location or device used.

Privacy and Monitoring

Users should have no expectation of privacy when using OCC equipment or systems. OCC reserves the right to access, monitor, and review information stored or transmitted through its systems for legitimate purposes, including but not limited to:

- Emergency resolution.
- System performance monitoring and security incident response.
- Internet usage monitoring, including remote access.
- Data backup and recovery operations.

Information may also be accessed or disclosed to external parties without prior notice when required for:

- Compliance with the New Jersey Open Public Records Act (OPRA).
- Response to valid subpoenas, court orders, or legal discovery requests.
- Internal or external audits, investigations, or inquiries.
- Execution of necessary business operations.

All electronic information created, stored, or transmitted using OCC systems is considered property of the College, unless explicitly stated otherwise.

Privileged Access

OCC IT personnel and other authorized users with elevated access privileges must exercise their roles responsibly. Access to user information is permitted only when:

- Required for system maintenance or security.
- Supported by adequate cause and reviewed by the appropriate College Officer or the IT Governance Committee.

Enforcement

Violations of this policy may result in disciplinary action, including revocation of access privileges, legal action, or other consequences as deemed appropriate by OCC.

Restricted Services

To safeguard OCC's sensitive information, the following services are restricted. This list is not exhaustive; users must exercise discretion when using any third-party technology not explicitly approved by OCC. When in doubt, consult OCC's Technology Department or IT Governance Committee.

Restricted services include:

1. **Social Media Platforms -** Personal or professional social media tools must not be used to store or communicate OCC information classified as confidential, private, or sensitive. Refer to the Social Media Policy for additional guidance.
2. **Third-Party Cloud Services -** Confidential OCC data must only be stored in OCC-managed cloud environments. Use of personal or external cloud storage solutions is prohibited unless explicitly approved by IT Governance.
3. **Third-Party Email Services -** OCC information classified as confidential or sensitive must not be transmitted or stored using non-OCC email services. Auto-forwarding to external email accounts is prohibited unless approved.

4. **Text Messaging (SMS/MMS) -** These services must not be used to transmit OCC confidential or sensitive information.
5. **Video Conferencing Tools -** Use is limited to OCC business and educational purposes. Users must ensure that sessions are configured to prevent unauthorized access to sensitive discussions or materials.
6. **Unapproved Chat Services -** OCC confidential or sensitive information must not be communicated or stored using chat platforms not approved by OCC IT.
7. **File Sharing Software (e.g., BitTorrent) -** Use of peer-to-peer file sharing software is prohibited unless explicitly approved for academic or business purposes by IT Governance.

Unauthorized Recording

The College prohibits the unauthorized recording of any work-related meeting, conversation, phone call, video call, or other form of communication. This includes audio, video, and screen recordings, as well as the use of any device or software designed to capture or store conversations. Employees may not record interactions involving coworkers, supervisors, students, vendors, or other members of the College community without prior authorization from Human Resources and the informed consent of all participants.

The College reserves the right to record meetings, training sessions, or other official events for legitimate business, academic, or compliance purposes. When the College initiates a recording, a message will be posted notifying all participants that the session is being recorded. Recordings will be managed in accordance with applicable laws and College policies.

This policy applies to recordings made on College-owned devices, personal devices, or any third-party platform. Violations may result in disciplinary action, up to and including termination.

Non-Compliance and Sanctions

Violation of this policy may result in disciplinary action, up to and including termination of employment, revocation of access privileges, and legal consequences. OCC reserves the right to investigate suspected violations and take appropriate action to protect its systems, data, and community.

ADOPTED: December 8, 1997
Revised: December 11, 2025