WILLIAM CAREY UNIVERSITY
OFFICE of INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

William Carey University provides faculty, staff and students with access to Information Technology (IT) Resources (as defined herein). Such access, when used appropriately, advances the university's mission by supporting teaching, learning, research, public service, and administrative activities. This Acceptable Use Policy (AUP) provides guidance for using IT resources.

This Acceptable Use Policy applies to all users of William Carey University's IT Resources whether affiliated with the university or not, and to all users of these resources from on campus or in remote locations. Users accept personal responsibility for the appropriate use of IT Resources. Each year, users will be required to review and accept the university's Acceptable Use Policy. Users accessing William Carey University IT Resources are responsible for maintaining a current understanding of the terms of this policy, which the university reserves the right to change without prior notice. The current version of this policy is available in the University's Policy and Procedures Manual. This policy also covers the use of all devices connected to the University IT Resources, whether owned by the university or private individuals.

While this policy deals specifically with issues involving the user of University IT Resources, it does not stand alone. All users of University IT Resources are expected to abide by the rules and regulations contained in applicable university handbooks, the Student Code, guidelines and policy and procedure manuals, as well as the laws of the State of Mississippi and of the United States of America. We remind users that the state and federal laws apply to the use of campus networks and the internet, including but not limited to those dealing with:

Copyright infringement	defamation	discrimination	fraud
Harassment	identity theft	obscene materials	records retention

POLICY

A. General

IT Resources are the property of the university and shall be used only for legitimate university instructional, research, public service, administrative, and approved contract purposes, except as allowed in this policy. Users are allowed to use IT Resources only to the extent authorized. When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced.

B. Responsibilities of users

1. Law and Policy

a. IT Resources must be used in compliance with applicable state and federal laws and university policies. IT Resources may not be used for any illegal purpose or activity or for any purpose which would violate university policy. Placing unlawful information or material on university systems is prohibited.
b. Downloading or disseminating copyrighted materials outside the provisions of "fair use" or without the permission of the copyright holder is prohibited. Illegally downloaded material may include, but is not limited to, music, movies, games, software, etc. Illegal use of peer-to-peer networking or other file-sharing technology is prohibited and may subject the user to civil or criminal penalties beyond penalties for violation of university policy.
c. Accessing or attempting to access computer systems through using IT Resources, including those external to the university, without authorization by the owner of that system, is specifically prohibited.
d. Sending electronic communication messages or creating web pages with fraudulent address or header information or containing misrepresentations in authorship or content in an attempt to deceive others is prohibited.
e. Using IT Resources in a way which would constitute a regular private business activity or which would violate the university's conflict of interest policies is prohibited.
f. Deliberately misusing trademarks in web pages and email, including university-owned marks such as the official logo or seal and trademarks owned by other entities is prohibited.
g. Providing false or misleading information in order to obtain access to computing or network facilities is specifically prohibited.

2. Accounts and Passwords

    a. Users are responsible for all activity originating from their accounts.
    b. Users must not divulge or make known their password(s) to any other person including, but not limited to, supervisors, coworkers, students, and IT staff members.
    c. Use of another user's account or identity is prohibited except by IT staff members during accountable impersonation for troubleshooting tasks and maintaining environment security as defined by specific job requirements.
    d. Any user who knows another user's password, intentionally or unintentionally, must notify the Office of Information Technology immediately.
    e. Falsifying or corrupting data in other's accounts, public directories, or a user's own stored documents is prohibited.
    f. Falsifying identity (including acting as another user with or without their knowledge) while using e-mail, student information systems, learning management systems, or any other IT resource is prohibited.

3. Respect for IT Resources, Users, and Information

    a. Users must respect the ability of other users to utilize IT Resources in an efficient and secure manner. Use of IT Resources shall not disrupt or distract from or interfere with the conduct of university business.
    b. Using any device or software which interferes with the ability of others to access IT Resources is prohibited.
    c. Damaging or attempting to damage any portion of IT Resources is prohibited.
    d. Deliberately introducing computer viruses, worms, or similar technologies which would harm the integrity of IT Resources, as well as attempting to create or disseminate such technologies, is prohibited.
    e. Deliberately misusing software or other techniques to degrade system or network performance or otherwise deprive authorized personnel of resources or access to university systems or networks, including techniques to disguise or obscure the source of data network traffic, is prohibited.
    f. Using IT Resources to release confidential, proprietary information, or information which has been classified as private, controlled, or protected without appropriate authorization is prohibited.
    g. Storing, transmitting, or processing any electronic data which includes student data or student records on systems or with software or services not approved by the Office of Information Technology is prohibited.
    h. Using university-licensed software and services in manners not approved by the Office of Information Technology is prohibited.

i. Licensing or procuring software, IT-related services, including but not limited to those related to hosting, streaming, eSignatures, forms, data collection, email delivery, scanning, encryption, data processing, statistics, research, testing, student monitoring, and security is prohibited.
j. Sending bulk electronic communication not approved by the Office of Information Technology is prohibited.
k. The privacy and rights of others must be respected. Monitoring or attempting to monitor another user's communications outside the scope of one's duties is specifically prohibited.

4. Incidental and Occasional Personal Use

a. Users may engage in incidental and occasional personal use of the university IT Resources provided that such use does not: Violate applicable law, rules and policies;

- Disrupt, distract from, or interfere with the conduct of university business;
- Involve regular private business activities; or
- Contravene supervisor direction regarding personal use of university IT Resources.

b. The use of social media services on university-owned equipment is prohibited except where required for university marketing and promotion as defined by specific job requirements.

C. Privacy

Electronic information on university networks or equipment, including but not limited to electronic communication, is subject to review, monitoring, copying, examination, and disclosure by the university as appropriate for legal, audit, or legitimate operational or management purposes. This includes, but is not limited to, the following:

1. It is necessary to maintain or improve the functioning of university computing resources;
2. There is reasonable cause for suspicion of misconduct under university policies or violation of state or federal laws;
3. It is necessary to comply with or verify compliance with federal or state law, including but not limited to software licensing agreements;
4. The requirements of maintaining a safe and secure network dictate the deployment of automatic security systems, such as host and network intrusion detection

systems, and active protection firewall systems designed to intercept, examine, and block data that threatens the university or external networks;

5. The university receives subpoenas or other court orders requiring disclosure of information; and
6. The university has notice of litigation or potential litigation.

The Systems Administrator, Chief Information Officer, and Director of Enterprise Services have the right to delete any file(s) belonging to faculty or staff who are no longer employed by the organization.

ENFORCEMENT

The university reserves the right to take appropriate actions reasonably necessary to protect the integrity and security of university computing facilities and data networks. This includes the right to immediately disconnect any computer disrupting the university data network; or being used for any activity in violation of this policy or other university policy or state and federal law.

DISCIPLINARY ACTION

The use of university IT Resources is a privilege that may be revoked at any time. Violation of this policy may result in discipline, up to and including termination or expulsion, in accordance with William Carey University policies. Legal action may also be taken when warranted. Violation of applicable laws may result in civil or criminal penalties.

DISCLAIMER

This policy does not preclude enforcement under the laws and regulations of the State of Mississippi and/or the United State of America. Internet access is also subject to the Acceptable Use Policies of those sites which a user may traverse. Any questions concerning ethical or legal use of computing facilities should be directed to the Chief Information Officer.

The university will not be responsible for damages resulting from the use or misuse of university computing and data network facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, hacking, or service interruptions caused by the negligence of an organization employee or by the user's error or omissions.

DEFINITIONS

A. **IT Resources:** Electronic processing, storage, and transmission systems, which include but are not limited to, the computers, terminals, printers, networks, copy machines, fax services, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the university. IT Resources also include, but are not limited to, institutional and departmental informational systems, faculty research systems, desktop computers, the university's campus network, and general access computer labs.

B. **Users:** All faculty, staff, administrators, students, consultants, guests, and any person or agency employed or contracted by the university or any of its auxiliary organizations who have a legitimate need to access IT Resources.
C. **Electronic Communication:** Email, text-messaging, instant messaging, and social networks.