OHIO CHRISTIAN
UNIVERSITY

Information Technology

1476 Lancaster Pike
Circleville, OH 43113
it.ohiochristian.edu
blazertech@ohiochristian.edu
740-420-5907

DOCUMENT #:POL-0002
EFFECTIVE: XX-XXX-2021
OWNER: ISO

ACCEPTABLE USE POLICY

CONTENTS

1.0 PURPOSE

Ohio Christian University's technology infrastructure exists to support the university and administrative activities needed to fulfill the university's mission. Access to these resources is a privilege that should be exercised responsibly, ethically, and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish each member of the university's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable Ohio Christian University to implement a comprehensive, system-wide Information Security Program.

2.0 SCOPE

This policy applies to all users of computing resources owned, managed, or otherwise provided by the university. Individuals covered by this policy include, but are not limited to, all workforce members and service providers with access to the university's computing resources and/or facilities. Computing resources include all Ohio Christian University owned, licensed, or managed hardware and software, email domains and related services, and any use of the university's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

3.0 PRIVACY

Ohio Christian University workforce members maintain no expectation of privacy while accessing, utilizing, transmitting, or storing information or communications on OCU systems [See employee handbook]. Additionally, in response to a judicial order or any other action required by law or permitted by official Ohio Christian University policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the university, the Executive Director of Information Technology may authorize an Ohio Christian University official or an authorized agent to access, review, monitor, and/or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the university's rules, regulations, or policy, or when access is considered necessary to conduct Ohio Christian University business due to the unexpected absence of an employee or to respond to health or safety emergencies.

4.0 POLICY

Activities related to Ohio Christian University's mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the university's mission is prohibited.

Following the same standards of common sense, courtesy, and civility that govern the use of other shared facilities, acceptable use of information technology resources generally respects all individuals' privacy, but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of Ohio Christian University's computing resources must adhere to the requirements enumerated below.

4.1 FRAUDULENT AND ILLEGAL USE

Ohio Christian University explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any of the university's information systems, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, users must not:

- Violate the rights of any individual or company involving information protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by Ohio Christian University.
- Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the university does not have a legal license.
- Export software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her manager immediately.

If any user creates any liability on behalf of Ohio Christian University due to inappropriate use of the university's resources, the user agrees to indemnify and hold the university harmless should it be necessary for Ohio Christian University to defend itself against the activities or actions of the user.

4.2 RESTRICTED INFORMATION

Ohio Christian University has both an ethical and legal responsibility for protecting restricted information in accordance with its Data Classification Policy. To that end, there are some general positions that the university has taken:

- Transmission of restricted information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is prohibited.
- The writing or storage of restricted information on mobile devices (phones, tablets, USB drives), removable media, and non-approved cloud storage is prohibited. These are not

acceptable storage locations unless an exception has been granted by the Executive Director of Information Technology.

- Mobile devices that access restricted information will be physically secured when not in use and located to minimize the risk of unauthorized access. Use by children (to play games, watch movies, etc.) on any device used to access Ohio Christian University's network, data, or systems is prohibited.
- All workforce members and service providers will use approved workstations or devices to access the university's data, systems, or networks. Non-university-owned workstations that store, process, transmit, or access restricted information are prohibited. Accessing, storing, or processing restricted information on home computers is prohibited.
- All company portable workstations will be securely maintained when in the possession of workforce members. Such workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use.
- Photographic, video, audio, or other recording equipment will not be utilized in secure areas.
- All restricted information stored on workstations and mobile devices must be encrypted.
- All workforce members who use university-owned workstations will take all reasonable precautions to protect the confidentiality, integrity, and availability of information contained on the workstation.
- University workforce members who move electronic media or information systems containing restricted information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized use.
- University workforce members will activate their workstation locking software whenever they leave their workstation unattended or will log off from or lock their workstation when their shift is complete.

4.3 HARASSMENT

Ohio Christian University is committed to providing a safe and productive environment, free from harassment, for all employees. For this reason, users must not:

- Use university information systems to harass any other person via e-mail, telephone, or any other means, or
- Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels he/she is being harassed through the use of the university's information systems, the user must report it, in writing, to his/her supervisor or any department head.

4.4 INCIDENT REPORTING

Ohio Christian University is committed to responding to security incidents involving personnel, university-owned information, or university-owned informational assets. As part of this policy:

- The loss, theft, or inappropriate use of university access credentials (e.g., passwords, key cards, or security tokens), assets (e.g., laptop, cell phones), or other information will be reported to the IT Help Desk.
- A university workforce member will not prevent another member from reporting a security incident.

4.5 MALICIOUS ACTIVITY

Ohio Christian University strictly prohibits the use of information systems for malicious activity against other users, the university's information systems themselves, or the information assets of other parties.

4.5.1 DENIAL OF SERVICE

Users must not:

- Perpetrate, cause, or in any way enable disruption of Ohio Christian University's information systems or network communications by denial-of-service methods
- Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system
- Intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system, or network

4.5.2 CONFIDENTIALITY

Users must not:

- Perpetrate, cause, or in any way enable security events, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access
- Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends
- Use the same password for Ohio Christian University accounts as for other non-Ohio Christian University access (for example, personal ISP account, social media, benefits, email, etc.)
- Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password
- Make copies of another user's files without that user's knowledge and consent unless required as part of an OCU role/function and only with the knowledge of management.

- Base passwords on something that can be easily guessed or obtained using personal information (e.g., names, favorite sports teams, etc.)

4.5.3 IMPERSONATION

Users must not:

- Circumvent the user authentication or security of any information system
- Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information
- Create and/or use a proxy server of any kind, other than those provided by Ohio Christian University, or otherwise redirect network traffic outside of normal routing with authorization
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

4.5.4 NETWORK DISCOVERY

Users must not:

- Use a port scanning tool targeting either Ohio Christian University's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of the Office of Information Technology conducting a vulnerability scan and appropriate staff utilizing tools in a controlled environment.
- Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the users unless this activity is a part of the user's normal job functions.

4.6 OBJECTIONABLE CONTENT

Ohio Christian University strictly prohibits the use of university information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be:

- Political
- Racist
- Sexually explicit
- Violent or promoting violence

Exceptions may be considered based on educational need and must follow the OCU exception process.

4.7 HARDWARE AND SOFTWARE

Ohio Christian University strictly prohibits the use of any hardware or software that is not approved by the Executive Director of Information Technology. Users must not:

- Install, attach, connect, remove, or disconnect hardware of any kind, including wireless access points, storage devices, and peripherals without the knowledge and permission of Information Technology
- Download, install, disable, remove, or uninstall software of any kind, including patches of existing software without the knowledge and permission of Information Technology
- Use personal flash drives or other USB based storage media without prior approval from management
- Take university equipment off-site without prior authorization.

4.8 MESSAGING

The university provides a robust communication platform for users to fulfill its mission. Users must not:

- Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism
- Send unsolicited electronic messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (spam)
- Create or forward chain letters or messages, including those that promote "pyramid" schemes of any type.

4.9 REMOTE WORKING

Remote working is at the discretion of OCU. Requests for alternate working arrangements must be made through and follow the Human Resources process. In addition, Human Resources must be notified if an employee is working from home on a normal basis without having completed the alternate working arrangements process.

When working remote, user must:

- Requests for alternate working arrangements must be made through supervision.
- Safeguard and protect any university-owned or managed computing asset (e.g., laptops and cell phones) to prevent loss or theft.
- Not utilize personally owned computing devices for Ohio Christian University work, including transferring Ohio Christian University information to personally owned devices unless approved by the Executive Director of Information Technology.
- Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing Ohio Christian University information processed, stored, or transmitted on university-owned assets.
- Not create or store restricted or private information on local machines or mobile devices.

- Only use approved methods for connecting to the university (e.g., VPN).
- Before taking any device used for connecting to university systems for service (even just screen replacement), notify Information Technology so appropriate steps can be taken to ensure all user accounts are disconnected.

4.9 OTHER

In addition to the other parts of this policy:

- Users must not use the university's information systems for commercial use or personal gain
- Users must not use the university's information systems to play games or provide similar entertainment
- Users must provide all encryption keys to Information Technology
- Information Technology must have a full access account on all systems not integrated with Active Directory.

5.0 ROLES AND RESPONSIBILITIES

Ohio Christian University reserves the right to protect, repair, and maintain the university's computing equipment and network integrity. In accomplishing this goal, Ohio Christian University IT personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by IT personnel about a user through routine maintenance of the university's computing equipment or network should remain restricted, unless the information pertains to activities that are not compliant with acceptable use of Ohio Christian University's computing resources.

6.0 ENFORCEMENT

Enforcement is the responsibility of the University's President or HR Director. Users who violate this policy may be denied access to the university resources and may be subject to penalties and disciplinary action both within and outside of Ohio Christian University. The university may temporarily suspend or block access to an account prior to the initiation or completion of disciplinary procedures when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of university computing resources or to protect Ohio Christian University from liability.

Users are subject to disciplinary rules described in the Employee Handbook and other policies and procedures governing acceptable workplace behavior.

7.0 EXCEPTIONS

Exceptions to the policy may be granted by the Executive Director of Information Technology or by his or her designee. All exceptions must be reviewed annually.

8.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- NIST 800-171
- FIPS-199
- Code of Ethics of the American Library Association

9.0 RELATED POLICIES

- Information Security Policy
- Data Classification Policy
- Data Classification and Handling Procedure

10.0 RESPONSIBLE DEPARTMENT

Information Technology

11.0 POLICY AUTHORITY

This policy is issued by Human Resources for Ohio Christian University.

12.0 REVISION HISTORY

Version	Date	Author	Revisions
1.0		Information Technology	Initial Draft

13.0 APPROVALS

Executive	**Information Security Officer**
Ted Perry	Amber Smith
CFO/COO	Executive Director of Information Technology
Date	Date
Signature	Signature