Albright College
Information Technology Services

IT Acceptable Use Policy

1. Purpose

The purpose of this Acceptable Use Policy (AUP) is to establish clear expectations for the responsible use of the organization's information technology (IT) systems, data, and digital resources. This policy aims to protect the organization, its employees, clients, and partners from security risks, legal exposure, and operational disruptions.

2. Scope

This policy applies to:

- All employees, contractors, consultants, temporary staff, and other users who access the organization's IT systems.
- All devices and equipment used to access organizational data or networks, including company-owned and personal (BYOD) devices where permitted.
- Any device acquired using Albright funds is considered property of Albright College.
- Any device provided to employees or installed throughout campus is explicitly recognized as Albright College property
- As the owner of its email systems, Albright College maintains ownership of all email content.

3. Acceptable Use

Users must:

1. **Use IT resources for authorized business purposes** unless limited personal use is explicitly permitted by management.
2. **Protect login credentials** and ensure passwords are kept confidential and follow the organization's password policy.
3. **Access only the systems and data for which they have authorization.**
4. **Comply with all applicable laws**, regulations, and contractual obligations.
5. **Use email, messaging, and collaboration tools professionally and respectfully.**

6. **Immediately report suspected security incidents**, data breaches, or policy violations to IT or Security.

4. Unacceptable Use

Users may **not**:

1. **Share passwords or allow others to use their accounts.**
2. **Restrict the use of Albright-issued laptops to authorized Albright staff only.**
3. **Attempt to bypass, disable, or interfere with security controls**, monitoring tools, or access restrictions.
4. **Install unauthorized software**, applications, or devices on organizational systems.
5. **Access, transmit, or store inappropriate, offensive, or illegal content**, including but not limited to pornography, hate material, or copyrighted materials without permission.
6. **Use IT resources for personal financial gain**, political activity, or external business interests unless specifically authorized.
7. **Engage in malicious activity**, including phishing, hacking, spreading malware, or any action that compromises network integrity.
8. **Connect unauthorized hardware**, including personal routers, USB drives, or IoT devices, to the organization's network.

5. Email and Communication Guidelines

Users must:

- Use corporate email accounts for business communications.
- Avoid opening suspicious attachments or clicking unknown links.
- Refrain from sending sensitive data without proper encryption or approval.
- Ensure communication complies with data protection and confidentiality requirements.

6. Internet Usage

Internet access is provided primarily for business use. Limited personal use is permitted if it:

- Does not interfere with work responsibilities.
- Does not violate this policy or any laws.
- Does not consume excessive bandwidth or system resources.

7. Data Protection and Privacy

Users must:

- Protect sensitive or confidential information from unauthorized access, disclosure, or alteration.
- Follow data classification, storage, and retention guidelines.
- Use only approved cloud services and storage systems for business data.

8. Device and Endpoint Security

- Devices must be secured with strong passwords or biometrics.
- Users must not disable antivirus software, firewalls, or security updates.
- Lost or stolen devices must be reported immediately.
- Personal devices (if allowed) must meet IT security standards.

9. Monitoring and Privacy

The organization reserves the right to:

- Monitor, access, and audit all IT systems, including email, internet usage, and stored data.
- Enforce this policy through technical and administrative measures.

Users should have no expectation of privacy when using organizational IT resources, except where prohibited by law.

10. Enforcement and Violations

Violations of this policy may result in:

- Revocation of IT access privileges
- Disciplinary action, up to and including termination
- Legal action if applicable

11. Acknowledgment

All users must acknowledge that they have read, understood, and agree to comply with this IT Acceptable Use Policy.