Acceptable Use Policy

Purpose and Scope

This policy defines acceptable use of company IT resources including computers, networks, email, internet, and software. All employees must comply.

Company resources are provided for business purposes. Limited personal use is permitted if it doesn't interfere with work or violate policies.

Prohibited Activities

Do not use company resources for illegal activities, harassment, discrimination, or accessing inappropriate content including pornography or hate speech.

Prohibited: Installing unauthorized software, attempting to bypass security controls, sharing credentials, or accessing systems without authorization.

Email and Communication

Company email is for business communication. Personal use should be minimal. All email is company property and may be monitored.

Use professional language and tone. Don't send confidential information to personal email accounts. Be cautious of phishing attempts.

Internet Usage

Internet access is provided for work-related research and communication. Streaming video or music should be limited to breaks and not impact bandwidth.

Don't visit malicious or inappropriate websites. Use company VPN when accessing company resources from outside networks.

Software and Applications

Only install software approved by IT. Unauthorized software may contain malware or violate licensing agreements.

Request software through the IT portal. Open source software requires security review before use. Keep all software updated.

Data and File Management

Store work files on company-approved cloud storage or network drives, not local devices. Follow data classification and retention policies.

Don't download or store illegal, offensive, or confidential content inappropriately. Regularly backup important files.

Mobile Devices

Company-issued mobile devices must have passcodes enabled and security software installed. Report lost or stolen devices immediately.

Personal devices accessing company email or data must comply with mobile device management (MDM) policies.

Monitoring and Privacy

The company reserves the right to monitor use of IT resources to ensure policy compliance and security. Employees have limited privacy expectations.

Monitoring may include email, internet activity, and file access. Monitoring is conducted in accordance with applicable laws.

Violations and Consequences

Policy violations may result in disciplinary action up to termination. Serious violations may be reported to law enforcement.

If you're unsure whether an activity is permitted, contact IT or your manager before proceeding.