



Ordinance No. 2026-217: Attachment A

Computer and Internet Use Policy

City of Madison, Alabama

Purpose

This policy establishes the standards and requirements for appropriate use of City-provided computers, internet access, networks, and related technology resources. It applies to all City employees who access City systems or networks. The objectives of this policy are to protect City data, maintain consistent security practices, ensure legal compliance, and support the effective delivery of City services.

Internet Access

Authorized Use

The City provides internet access to employees for the primary purpose of conducting official City business and supporting day-to-day operations. Access to the internet is granted and managed by the IT Department in accordance with each employee's job responsibilities and operational needs. The IT Department reserves the right to monitor, restrict, modify, or revoke internet access at any time to ensure network security, maintain system performance, and protect City resources.

Prohibited Activities

Employees must use City internet access responsibly and, in a manner, consistent with the professional standards of the City. Personal internet use should be conducted through the City's designated public Wi-Fi network whenever possible and should not utilize the City's internal network, systems, or resources unless authorized for legitimate City business purposes.

The following activities are strictly prohibited:

- Accessing, viewing, downloading, or storing websites, files, or images containing offensive or inappropriate content that is unrelated to City business, unless specifically required for authorized City purposes.
- Using City internet resources for personal business, commercial activity, or personal financial gain
- Streaming media, gaming, or other high-bandwidth personal activities during work hours
- Bypassing or attempting to circumvent City network security controls or content filters
- Casual browsing of restricted, sensitive, or unauthorized data

File Access Outside of Job Scope

If an employee encounters system access that exceeds their authority or job scope, they must immediately notify the City of Madison Information Technology (IT) Department and document when, where, and how the access occurred.

Monitoring and Privacy

Notice: Internet Activity Is Logged and Monitored

All internet activity conducted on City networks, including visits to linked or redirected websites, is logged and monitored by the City's internet access systems. While the City does not routinely audit individual usage, it reserves the right to review activity in specific cases. Law enforcement agencies may examine internet activity as part of civil or criminal investigations, and the City reserves the right to disclose relevant internet activity to law enforcement officials upon lawful request.

Any violation of this policy, including abuse or misuse of internet access, may result in disciplinary action, up to and including termination of employment.

Access Agreement

No employee may be granted authorized internet access until they have received, reviewed, and agreed in writing to comply with this policy. A signed copy of the acknowledgment form will be retained in the employee's personnel file and must be renewed upon any significant policy update.

Computer Use

Approved Software

All City computers and workstations are subject to unannounced audits at any time. Only software that has been reviewed and approved by the City of Madison IT Department may be installed on City-owned equipment. Employees are strictly prohibited from installing personal applications, games, browser extensions, or any unauthorized software on City devices.

Virus and Security Protection

Employees must report any suspected issues with anti-virus or endpoint security software to IT personnel immediately. Employees should exercise caution when uploading files, opening email attachments, or downloading content to City computers or servers, as these are common vectors for malware and ransomware.

Technical Support

All technical support, system configuration, and equipment maintenance must be performed by, or under the direction of, City of Madison IT personnel. Employees are not authorized to independently modify, repair, or reconfigure City-issued computer equipment, software settings, or network connections. Unauthorized changes may void manufacturer warranties and create potential security risks for City systems.

Employees must submit all requests for assistance through the designated IT help desk process to ensure timely and proper support.

Personal Computers on City Property

Unless approved by IT, personally owned computers, laptops, tablets, and other portable devices are not permitted to connect to City networks.

This restriction exists to protect the integrity of City systems, prevent unauthorized access and potential data breaches, maintain consistency in software versions and security configurations, and support the IT Department's ability to monitor and manage all devices connected to City infrastructure effectively.

External Devices and Network Equipment

External Storage Devices

Unless approved by IT, personal external storage devices, including USB flash drives, portable hard drives, and other storage devices, are not permitted on the City network. Approved devices must be scanned by IT personnel before they're connected to any City computer. Employees are prohibited from using personal storage devices to copy, transfer, or remove City data unless they have received prior authorization.

Wireless Equipment

Unauthorized wireless access points, routers, and any other network devices are strictly prohibited on City networks under all circumstances.

All network equipment must be installed, configured, secured, and managed exclusively by the IT Department. Employees are not permitted to add, connect, modify, troubleshoot, or reconfigure any network infrastructure or related devices.

Access Upon Separation from Employment

Upon separation or suspension from City employment for any reason, the individual's authorization to access City computer systems, networks, and data will be immediately revoked. Human Resources is responsible for notifying IT personnel as soon as an employee's separation date is known, and no later than the employee's last day of work.

IT personnel will promptly revoke, suspend, or change the individual's access credentials, including account passwords, access codes, system permissions, and email access. All City-issued equipment must be returned on or before the employee's last day.

Authorized System Use and Misuse of Access

City-provided systems, software, and data are to be used strictly for the performance of an employee's assigned job duties. Access to City systems is granted based on an employee's role and the specific responsibilities of their position. Employees must not use any City system, application, or data in a manner that falls outside the scope of their authorized job functions, regardless of whether the system itself is otherwise accessible to them.

The following actions are expressly prohibited and constitute misuse of authorized access:

- Using City systems or software to perform transactions, process payments, register individuals, or conduct any activity that is not part of the employee's assigned duties or that confers a personal benefit to the employee or others outside of official City business
- Forwarding, copying, or transmitting City data, records, or confidential information to personal email accounts, personal storage devices, or any destination outside of City-approved systems

- Accessing, modifying, or extracting records, accounts, or information belonging to individuals or departments outside the employee's authorized scope of work
- Using City systems to conduct activity that benefits the employee personally, financially, or professionally outside of their official City role
- Sharing login credentials or granting system access to individuals who are not authorized to use that system, including other City employees whose job functions do not require such access

Employees who are unsure whether a specific action is within the scope of their authorized access must consult their supervisor or the IT Department before proceeding. The ability to access a system does not imply authorization to use it for any purpose beyond an employee's assigned duties.

Compliance and Enforcement

All employees and authorized users are expected to comply fully with this policy. Violations may result in disciplinary action, up to and including termination of employment, civil or criminal legal action, and permanent revocation of access to City systems and data.

All employees are expected to cooperate fully with any authorized audit, investigation, or review related to City technology use. Employees who become aware of a potential policy violation by another individual are encouraged to report it to their supervisor, the IT Department, or Human Resources.