Acceptable Use Policy (AUP)

Section 1. Application

This policy applies to any county, state employee, contractor or third party, who uses any device, whether county or state owned, to connect to the Montgomery County or State networks.

Section 2. Requirements

1. Users may not connect personal devices to the Montgomery County Network(s) without express written permission from the department head to the Montgomery County IT Director. This requirement does not apply to users who connect to the Montgomery County network(s) through a county-supplied "guest" Wi-Fi network.
2. Personally owned "smart" devices may not be connected to the county networks. "Smart" devices, commonly referred to as the "Internet of Things," include smart thermostats, smart appliances, or wearable technologies.
3. All devices connected to the county Network(s) must have updated malware/anti-virus protection.
4. Users must not attempt to access any data, documents, email correspondence, and programs contained on systems for which they do not have authorization.
5. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
6. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes.
7. Users must not use their county or state credentials, e.g., .gov email addresses, for non-official tasks.
8. Users must not make unauthorized copies of copyrighted, county or state-owned software.
9. Users must not download, install, or distribute software to county owned devices unless it has been approved by the IT Director.
10. Users must ensure all files downloaded from an external source to the county Network(s) or any device connected to the county Network(s) including a diskette, compact disc (CD), USB flash drive, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.
11. Users must ensure that the transmission or handling of personally identifiable information (PII) or other restricted or highly restricted data is authorized and encrypted.
12. Users must not download Montgomery County or State data to personally owned devices unless approved by the Montgomery County Manager, or IT Director.

13. Users must comply with the Data Retention Guideline for local government agencies located at https://archives.ncdcr.gov/government/local ***Note**: Per the NC Department of Natural and Cultural Resources (DNCR), OneDrive for Business: Best Practices and Usage, "OneDrive for Business is not intended for permanent storage of public records."* See https://archives.ncdcr.gov/government/digital-records/digital-records-policies-and-guidelines/microsoft-365-best-practices-and-usage. Long-term storage and collaboration efforts must utilize other available tools, e.g., Microsoft SharePoint.
14. Users must not purposely engage in activity that is illegal according to local, state or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store, or transmit material which may be deemed to be offensive, indecent or obscene such as racial or sexually explicit materials
15. Users accessing the Montgomery County Network(s) through a Local Area Network (LAN) must avoid unnecessary network traffic and interference with other users. Specific prohibitions include, but are not limited to, the following:

    (a) Unsolicited commercial advertising by public employees and Montgomery County Network(s) users. For this policy, "unsolicited commercial advertising" includes any transmission initiated by a vendor, provider, retailer, or manufacturer of goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer that describes goods, products, or services. This prohibition does not include the following:

    (i) discussions of a product or service's relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer, or manufacturer, or related to or affiliated with the vendor, provider, retailer, or manufacturer)

    (ii) responses to questions, but only if such responses are direct replies to those who inquired via electronic mail

    (iii) mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.

    (b) Any other type of mass mailing by employees and others accessing the Montgomery County Network(s) through the county LAN that does not pertain to governmental business or a state-sponsored activity.
16. Users accessing the Montgomery County Network(s) through the county LAN must only access Internet-streaming sites consistent with the mission of the county for the minimum amount of time necessary.
17. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user of access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
18. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved in writing by the County Manager or IT Director.

19. Users must not operate any utility, application, or service that would obfuscate or anonymize user or device identity (e.g., IP address, MAC address, user identity, geographic location, etc.). Such services include, but are not limited to, the following: personal VPN, Private Relay, and Tor.
20. Information technology resources must not be used for personal benefit, e.g., gambling, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state, or federal law.
21. Access to the Internet from county-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to utilize the county equipment in any fashion.
22. Users must report any weaknesses in computer security to the IT department for follow-up investigation. Weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.
23. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy.
24. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of information.
25. Users should not use **unauthorized** Cloud Services (e.g., file storage/sharing services like DropBox, Google Drive, etc.) for sharing of state data.
26. Users must not send county or state data to non-authorized individuals or accounts or services via an auto-forwarding capability. The forwarding of county or state data must comply with the measures outlined within this policy.

Section 3. Incidental Use

County and State systems are intended for primarily business purposes, but limited (incidental and occasional) personal use may be permissible when authorized by your management and it does not do the following:

1. Interfere with the normal performance of an employee's work duties.
2. Resulting in direct costs to the county, causes legal action against, or causes embarrassment to the county. Departments should restrict incidental personal use of email, internet access, printers, copiers, and any other information technology resources to employees.
3. Involve interests in personal or outside business and/or other non-authorized organizations and activities such as selling or soliciting personal property/items, promoting commercial ventures, charitable, religious, or political activities.

Section 4. Violations

Violation of this policy could result in disciplinary action, termination, loss of information resources, and criminal prosecution.

Section 5. Acknowledgement of Policy

Montgomery County employees, contractors, and interns must acknowledge in writing that they have received a copy of this policy.

I have read, understand, and will abide by the above Acceptable Use Policy when using computers and other electronic resources owned, leased, or operated by the county. I further understand and will abide by the above Acceptable Use Policy when using personal computing devices not owned, leased, or operated by the County agencies. I further understand that I have no expectation of privacy when connecting any device to the Montgomery County Network(s) and that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation of this policy, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

_____ _____

Name *Date*

_____

User Signature