# Arapahoe County Acceptable Use Policy

1. **Purpose.** The purpose of this policy is to outline the acceptable use of technology — including, but not limited to, computers, hardware, software, applications (including Software-as-a-Service [SaaS], web-based platforms, low-code/no-code platforms, and Artificial Intelligence [AI] tools) network, internet, email, phones, remote access, and other computing devices — at Arapahoe County. Inappropriate use exposes Arapahoe County to unnecessary risks.

2. **Scope.** This policy applies to the use of County Computing Resources. County Computing Resources include all computers and other computing devices, cell phones and other mobile devices, servers, cloud storage, applications (including web-based, SaaS, low-code/no-code platforms and Artificial Intelligence [AI] tools), as well as all other network hardware and software resources utilized to conduct Arapahoe County business or interact with internal networks and business systems, that are owned, leased, or subscribed to by Arapahoe County, its elected and appointed officials, full and part-time employees, volunteers, contractors, and agents.

3. **Policy**
    a. **General Use and Ownership**
        i. Information stored on County computing resources — whether owned, leased, or subscribed to by Arapahoe County — remains the property of the County. Users have no expectation of privacy when using County technology. Electronic communications related to County business, including those sent from personal devices, are County records subject to monitoring and the Colorado Open Records Act (CORA, C.R.S. § 24-72-201 et seq.). Arapahoe County proprietary information must be protected in accordance with the Data Protection Standard (Section 7).
        ii. Theft, loss, or the unauthorized disclosure of Arapahoe County proprietary information, user credentials or equipment must be promptly reported to the appropriate supervisor/manager and the Information Technology Department within 24 hours. Theft or unauthorized disclosure of information in or on County Computing Resources may result in corrective action up to and including termination. In addition, the County may pursue all other remedies available to it at law.
        iii. County Computing Resources may be accessed, used, or shared only to the extent it is authorized and necessary to fulfill assigned job duties.
        iv. Limited, incidental personal use of County computing resources is permitted. The Information Technology Department will monitor, may restrict, or revoke access at any time to enforce County policy and protect County systems. Prohibited activities include, but are not limited to, cryptocurrency mining or trading, gaming, gambling, and any illegal, inappropriate, or high-risk activities. Unapproved video and audio streaming is also prohibited. Users have no expectation of privacy when using County computing resources. Violations may result in corrective action.
        v. Authorized individuals, within Arapahoe County, can and will monitor County Computing Resources and network traffic at any time for security and network maintenance purposes. This includes continuous monitoring of internet traffic and websites visited. The County's Information Technology Department does block certain categories of websites from County traffic.
        vi. Arapahoe County reserves the right to audit networks and systems on a periodic

basis to ensure compliance with this policy, licensing requirements, and appropriate use. This includes all applications, software, SaaS solutions, web-based platforms, low-code/no-code platforms and AI technologies used to conduct County business.

vii. With approval by the County Attorney's Office and Human Resources, employee files and data may be made available for business/legal reasons.

viii. Employees accessing County Computing Resources and processes must safeguard their device(s) from loss or theft.

**b. Security and Proprietary Information**

i. All mobile (e.g., cell phones, tablets) and computing devices that connect to the internal network must comply with the Minimum Access Provisions (Section 6) of this Policy.

ii. System level and user level passwords must comply with the password requirements established by the Information Technology Department.

iii. Providing network, computer, or system access to another individual, deliberately or through failure to secure access appropriately, is prohibited.

iv. All computing devices and cell phones are to be secured with a password-protected screensaver or auto-locking feature with the automatic activation set to 20 minutes or less, unless otherwise approved.

v. Systems must be locked, logged off, or rebooted when the device is unattended.

vi. Employees must exercise extreme caution when opening e-mail attachments received from unknown senders. Any suspicious messages, errors, or behavior must be reported immediately to the Information Technology Service Desk.

c. **Low-Code and No-Code Application Development**

Arapahoe County permits the use of low-code and no-code platforms that are part of the County's authorized services and application portfolio to improve business processes and operational efficiency. The use of any low-code or no-code platform outside of the County's portfolio and not explicitly reviewed and approved by Information Technology (IT) is prohibited.

The following requirements apply:

i. Employees, contractors, volunteers, and affiliates may not run applications and integrations using low-code or no-code platforms to build persistent solutions without prior review and approval from the Information Technology (IT) Department.

ii. Requests to develop solutions using low-code or no-code platforms must:

- Be reviewed and approved by the Information Technology (IT) Department prior to development or deployment.
- Clearly described the business purpose of the tool, the data it will use, and how it will be supported.
- Comply with County policies related to cybersecurity, data privacy, records retention (if applicable), and accessibility.
- Follow IT-defined standards for user access, ownership, and continuity of operations.

iii. The Information Technology (IT) Department must approve:

- The platform used and authorized use;
- Administrative or elevated access;
- Connections to County systems, County data, or third-party services;
- Deployment and ongoing operation.

iv. Applications or integrations created, deployed, or used without IT review and approval may be suspended, restricted, or removed.

v. The Information Technology (IT)Department may assume administrative control of approved applications to ensure continuity of operations, compliance with County standards, and proper risk management.

d. Any new or modified technology procured by the County—including applications, Software-as-a-Service (SaaS) products, enhancements or new products provided by existing County vendors, web-based platforms, Artificial Intelligence (AI) tools, and low-code or no-code development platforms—intended to provide, support, or deliver services to County residents or employees must be reviewed and approved by the Information Technology (IT) Department for security, compliance, and accessibility prior to procurement, development, deployment, or use.

4. **Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

Under no circumstances is an employee of Arapahoe County authorized to engage in any activity that is illegal under local, state, federal, or international law while using Arapahoe County-owned resources.

The activities referenced in Section 4.a and Section 4.b are not an exhaustive list but attempt to provide examples of activities which fall into the category of unacceptable use.

a. **Computer, Mobile Device, System, and Network Activities** The following activities are strictly prohibited:

i. Violations of the rights of any person or company protected by copyright, trade secret, trademark, patent, 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 Arapahoe County.

- Downloading or installing free software, or using free or unmanaged services, due to potential security, licensing, and data protection risks. Such software or services may introduce malware, unauthorized data sharing, or license violations. If software or services are required for County business, employees shall contact the Information Technology (IT) Department for review and pre-approval.

ii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copy-righted sources, copyrighted music, and the installation of any copyrighted

software for which Arapahoe County or the end user does not have an active license.

iii. Accessing data, a server, or an account for any purpose other than conducting Arapahoe County business, even if the user has authorized access.
iv. Exporting or sharing software, technical information, network diagrams, internal procedures, encryption software, or technology in violation of international or regional export control laws, is illegal and/or not permitted. The IT Director and/or the County Attorney's Office must be consulted prior to supplying any material that is in question.
v. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.), whether intentionally or inadvertently.
vi. Revealing one's account password or allowing use of one's account by others is prohibited. This includes family and other household members when work is being done at home.
vii. Using County Computing Resources to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
viii. Making fraudulent offers of products, items, or services originating from any Arapahoe County account.
ix. Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
x. Port scanning or security scanning unless prior written approval by Arapahoe County's Information Technology (IT) Department is obtained.
xi. Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
xii. Circumventing user authentication or security of any host, network, or account.
xiii. Introducing honeypots, honeynets, malware or similar technologies on the Arapahoe County network or computing devices.
xiv. Connecting any devices to the Arapahoe County network without authorization from the Information Technology (IT) Department is prohibited. The Guest Wireless network may be used without such authorization.
xv. Interfering with or denying service to any user (for example, denial of service attack).
xvi. Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
xvii. Providing information about, or lists of, Arapahoe County employees to parties outside Arapahoe County unless specifically authorized by the County Attorney's Office.
xviii. Procuring, developing, or operating unapproved applications, web-based services, Software-as-a-Service (SaaS) platforms, Artificial Intelligence (AI) systems—including AI chatbots, assistants, automated decision-making tools,

and low-code or no-code platforms—intended to provide, support, or deliver services to the County residents, or County employees without prior review and approval by the Information Technology (IT) Department.

b. **Email and Communication Activities.** When using County Computing Resources to access and use the Internet, users must realize they represent the County. Questions should be addressed to the Information Technology Department. The following are prohibited:

i. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
ii. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
iii. Unauthorized use, or forging, of email header information.
iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
vi. Posting via email or chat the same or similar non-business-related messages to large numbers of users.

**5. Policy Compliance**

a. *Compliance Measurement.* The Arapahoe County Information Technology (IT) Department will verify compliance with this policy through various methods, including but not limited to system reports, internal and external audits, and license or hardware audits, and will report findings to the Information Technology Director as the policy owner. This may include monitoring and auditing application usage, websites visited, SaaS subscriptions, web-based services, and AI implementations to ensure adherence to County security, privacy, accessibility, and ethical standards.
b. *Exceptions.* Any exception to the policy must be approved in advance and in writing by the Arapahoe County Information Technology (IT) Department Director and, where applicable, the County Attorney's Office.
c. *Non-Compliance.* An employee found to have violated this policy may be subject to corrective action, up to and including termination of employment.

**6. Minimum Access Provisions (MAP)**

a. The principle of least privilege states that users, systems, and processes only have access to resources (networks, systems, and files) that are necessary to perform their as-signed function. By governing the level of access for each user, system, and process, the principle of least privilege limits the potential damage posed from unsanctioned activities, whether intentional or unintentional.
b. The Information Technology (IT) Department will work with each department or office Security Administrator to determine what the appropriate level of security and access for any given user should be, following the MAP principle.
c. For internal Information Technology access to systems, e.g., domain administrator accounts, the MAP principles will also be applied and secondary accounts and credentials, distinct from the IT user's primary account, will be utilized.

**7. Data Protection Standards**

a. Users shall comply with all data protection controls/requirements and shall not

transmit or store another party's Personal Identifiable Information (PII), regulated, or confidential information in an unencrypted form or in any application, service, or system not sanctioned by the Information Technology (IT) Department. This includes, but is not limited to, emailing such information internally or externally, or uploading it to unsanctioned SaaS or web-based platforms.

i. Personal Identifying Information (PII) is a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in CRS Section 24-73-103(1)(a); an employer, student, or military identification number; or a financial transaction de-vice, as defined in CRS Section 18-5-701(3).

ii. When no longer needed for business reasons and when all applicable retention periods have expired, PII shall be deleted from all County Computing Resources in accordance with each Department's/Office's retention policy, as defined by and in accordance with State law.

b. Users shall password protect all County Computing Resources that are used to access County information and that are connected to the County IT infrastructure, whether within County facilities or remotely connected. This includes access to cloud-based services that the County utilizes, e.g., Microsoft Office365.

c. Users may learn, or have access to, sensitive information concerning County and/or department/office business, Arapahoe County residents and employee data. It is the responsibility of users to maintain the confidentiality of all County information. Users must take precautions to protect the unauthorized or careless disclosure of this information.

d. No sensitive data, including PII and HIPAA protected information, shall be downloaded or stored on a personal IT resource, including personal portable devices, computers, external hard drives, CDs/DVDs, or USBs.

e. As a public entity, Arapahoe County is subject to specific open records provisions of Colorado and Federal law. These data protection standards do not exempt an employee or the County from those open records provisions. See, County Public Records Policy and Section 10, below.

f. All sensitive data stored on portable devices — laptops, tablets, external hard drives, etc. — is to be encrypted or the entire storage device shall be encrypted.

g. All SaaS and web-based applications, including AI applications that store, process, or transmit County data — particularly Personal Identifiable Information (PII), regulated, or confidential information — must be reviewed and sanctioned by the Information Technology (IT) Department and comply with the County's Data Protection Standards and applicable state and federal privacy laws.

**8. Remote Access (Connecting to the County Network/Systems from outside County facilities)**

a. Remote access users shall connect to Arapahoe County IT infrastructure exclusively through the County-approved Virtual Private Network (VPN) solution when accessing internal applications, as authorized and managed by the Information Technology (IT) Department.

b. Remote access users shall ensure that both County Computing Resources and personally owned technology assets used to connect to the County IT infrastructure are password protected and use up-to-date operating system software and security software (i.e., anti-virus, anti-spyware, firewall, and host intrusion prevention).

c. County Computing Resources that are lost or stolen must be reported to the employee's

manager and the Information Technology Service Desk (ITServiceDesk@arapahoegov.com) within 24 hours.

d. The County reserves the right to remotely wipe any device, including an employee-owned device if it was used to access County resources, if necessary, to protect the security, confidentiality, and integrity of County data.
e. Data on devices pertaining to County business, including employee-owned devices, is subject to the Colorado Open Records Act (CORA).

**9. Computer Hardware, Software, Software as a Service Subscriptions, Web-Service Subscriptions and Information Communication and Technology (ICT) Procurement**

All County Information and Communication Technology (ICT) — including hardware (such as desktop and laptop computers, servers, routers, switches, firewalls, monitors, and printers), software, subscriptions, platforms, cloud services, Artificial Intelligence (AI) systems, integrations, and professional technology services — that is procured using County funds and used to provide, support, or deliver services to County employees or residents must be reviewed and approved by the Information Technology (IT) Department for security, compliance, and accessibility, prior to purchase, subscription, renewal, development, deployment, or use.

a. Requests for computer and tablet hardware and software are to be sent to the appropriate asset manager, who will obtain quotations, and will then arrange for the purchase.
b. Departments and Offices are responsible for cell phone procurement and cell phone plan subscriptions.
c. Keyboard, mouse, and headset purchases are exempted from this policy and may be procured directly by the Department or Office.
d. Any hardware and software purchases made outside of this policy will be the financial responsibility of the purchaser, not the County.
e. The procurement of subscriptions and professional technology services are included in this policy and must be reviewed and approved by the Information Technology (IT) Department to verify appropriate licensing, data usage and retention, and cybersecurity measures.

**10. Data Ownership/Privacy/Public Records**

All information or data contained or stored in or on any County Computing Resource including email and data created, processed, or stored through SaaS, web-based, or AI technologies is the property of Arapahoe County. Any information or data contained or stored in or on any County Computing Resources is always available to the County and its authorized elected and appointed officials, employees, agents or other representatives, and employees, officials and other users shall have no expectation of privacy with respect to such information or data. All employees and officials should be aware that information and data contained on computers, cell phones, and their correspondence in the form of e-mail or messaging systems, may be considered a public record under public records law and may be subject to public inspection pursuant to the Colorado Open Records Act, C.R.S. 24-72-201, et seq. The Arapahoe County Information Technology Director is the official custodian of e-mail and other electronic messages. If such information is requested and it is determined that it is a public record available for inspection, it will be released for public review. Please refer to the County's current Public Records Policy for more information regarding public records requests.

**11. Complaint Procedures**

To report a violation, employees should contact their supervisor and/or manager who should report it to the appropriate official. The responsible department director/elected official shall then take appropriate action. Alternative avenues for reporting include Human Resources and the "Ethics Hot line".

**12. Related Standards and Policies**

a. Social Media Policy: Social Media Policy.pdf
b. Mobile Device Policy: Mobile Device Policy.pdf
c. Cell Phone Policy: Cell Phone Policy.pdf
d. Ethical Artificial Intelligence Policy Ethical Artificial Intelligence.pdf

**Examples of Permissible Uses of Arapahoe County Computing Resources**

- Day-to-day functions as outlined by the employee's written job descriptions, the supervisor/manager, or by the governing body that oversees the employee's department.
- Disseminating appropriate County documents to other individuals or organizations.
- Communicating with other County employees.
- Obtaining information from job-related vendors on products and services.
- Applying for or administering grants or contracts for County Government research or programs.
- Communication with members of professional organizations, collaborating on articles and other writing, reviewing information on career and educational opportunities, and participating in reading electronic discussion groups on professional or career development topics.
- Training to enhance business and/or technical skills, pertaining to the employee's job function or as assigned by the employer.
- Sending messages to large distribution lists (e.g., department-wide or county-wide lists) when there is clear and legitimate business need to notify all recipients, in compliance with County messaging and communication standards. Approval for access to large distribution lists must be granted by the Information Technology Director.
- Bulk or mass messaging to large recipient lists external to the County (e.g., 400 or more recipients), must be conducted using a County-approved bulk email or messaging platform and coordinated with Information Technology.
- County-procured subscriptions to Software-as-a-Service (SaaS), web-based, or AI-enabled services intended to provide, support, or deliver services to County residents or County employees—beyond tools used solely to support an individual's internal job functions—must be reviewed and approved in advance by the Information Technology (IT) Department to ensure compliance with security, data protection, ethical AI use, and accessibility requirements.
- Reasonable incidental personal communications or transactions, so long as it does not interfere with the conduct of Arapahoe County Business, incur additional system costs, interfere with the employee's duties, or violate any other County policy, procedure, or departmental standard.

**Examples of Prohibited Uses of Arapahoe County Computing Equipment**

- Sending broadcast messages or mass file attachments for personal use. This includes the sale of any personally owned item or school fundraisers, etc. It is suggested that the employee instead use the Classified Ads on the Intranet.
- Sending email to "all employees" either with or without using one or more distribution lists unless approved by the Director of Information Technology. Mass employee communications should be coordinated through the county's communication services division unless emergent needs to dictate an alternative approach.

- Subscribing to, procuring, implementing, or using any application, service, Software-as-a-Service (SaaS) platform, web-based tool, Artificial Intelligence (AI) technology, or other technology solution that has not been reviewed and approved by the Information Technology (IT) Department is prohibited when the technology is intended to provide, support, or deliver services to County employees or County residents.
- Use of the County's e-mail system for any illegal activity including, but not limited to, gambling, child or other pornography, solicitation to distribute or purchase controlled substances, etc.
- Messages or internet content containing sexual implications, racial slurs, gender-specific comments, or any comment that offensively addresses someone's age, religious or political beliefs, national origin, or disability, unless associated with a current public safety investigation.
- Use of electronic communications to be used to send or receive copyrighted materials, trade secrets, proprietary financial information, chain letters or similar materials.

**Glossary**

**Acceptable Use Policy (AUP)**
A policy that defines permitted and prohibited use of County computing resources to ensure security, compliance, and operational integrity.

**Application**
A business application is a persistent workspace designed to manage repeatable processes or workflows over time. Unlike a tool that simply presents information or answers a one-time question, an application enables users to create, update, and store data, serving as a functional source of truth that supports and guides tasks from start to finish across multiple, sessions or users.

**Artificial Intelligence**
Systems or tools that perform tasks typically require human intelligence, including but not limited to chatbots, virtual assistants, code generation tools, content generation tools, and automated decision-making systems.

**Bulk Messaging**
The distribution of messages to many recipients (e.g., 400 or more) on a recurring basis, including email or other electronic communication platforms.

**County Computing Resources**
Any technology resource owned, leased, licensed, or managed by the County, including laptop, desktop, and mobile devices, tablets, iPad's, networks, applications, SaaS platforms, cloud services, and AI technologies.

**County Data**
All information created, received, maintained, or transmitted in the course of County business, regardless of format or storage location.

**Information Communication Technology (ICT)**
All technologies used to create, store, process, transmit, or exchange information, including computing devices, networks, applications, SaaS platforms, web-based services, telecommunications systems, and AI technologies.

**Information Technology Department**

# Arapahoe County Acceptable Use Policy

The County Information Technology department is responsible for approving, securing, monitoring, and enforcing the use of County computing resources.

**Low-Code / No-Code Platforms**
Application development platforms that allow users to create applications, workflows, automations, or integrations using graphical interfaces, configurations, or minimal programming. Examples include tools used for process automation, forms, dashboards, and system integrations.

**Personal Identifiable Information (PII)**
Information that can be used to identify an individual, either directly or indirectly, such as name, address, Social Security number, driver's license number, or similar data elements.

**Minimum Access Provision (MAP)**
The principle that users are granted the minimum level of access is necessary to perform their assigned job duties, consistent with business need, security requirements, and risk management practices.

**Remote Access**
The ability to connect to County systems from outside County-controlled facilities using approved and secure access methods.

**Sanctioned/Approved**
Reviewed and formally authorized by the Information Technology (IT) Department for business use, security, compliance, accessibility, and ethical considerations.

**Software as a Service (SaaS)**
At its core, **SaaS (Software as a Service)** is a way of delivering applications over the internet as a service. Instead of installing and maintaining software on your individual computer or a local office server, you simply access it via the web. Examples include but are not limited to, Tyler Technologies, Granicus, PowerDMS/NEOGOV, CentralSquare, SAP.

**Unauthorized Use**
Any use of County computing resources that is not explicitly permitted by this policy or approved by the Information Technology (IT) Department.

**Revision History**

| Date | Revision # | Revision Type | Author |
|---|---|---|---|
| 05/12/2021 | AUP-1.0 | E-Team presentation | David Bessen |
| 10/31/2025 | AUP 2.0 | Additions | Nikki Rosecrans |
| 01/09/2026 | AUP 2.1 | Editions | Nikki Rosecrans |
| 03/15/2026 | AUP 2.1.1 | Editions | Nikki Rosecrans |