Arapahoe County Acceptable Use Policy for Computers and Related Technology

1. **Purpose.** The purpose of this policy is to outline the acceptable use of technology—including, but not limited to, computers, hardware, software, 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, 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, the employee, or a third party, remains the sole property of Arapahoe County and is subject to monitoring at any time. See, Section 10. Proprietary information must be protected through legal or technical means in accordance with the Data Protection Standard provisions specified in 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 in a timely manner. 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. Although employees may use County Computing Resources for incidental personal use, they are responsible for exercising good judgment regarding the personal use of County Computing Resources and internet usage and shall have no expectation of privacy. Individual departments or offices may create additional guidelines concerning personal use. In the absence of such guidelines, employees should consult their supervisor or manager.
        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 any networks and systems on a periodic basis to ensure compliance with this policy, licensing, and appropriate usage.
        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 shutdown 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.

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.
    - The downloading and installation of free software or utilizing free services is not permitted, as it may violate applicable license agreements. If such software or services are needed, please contact the Information Technology Department.
ii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted 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 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 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.

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 Department will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, license audits, hardware audits and feedback to the Policy owner.
b. *Exceptions.* Any exception to the policy must be approved in advance and in writing by the Arapahoe County Information Technology 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 assigned 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 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 follow all data protection requirements and will not disseminate Personal Identifying Information (PII), regulated or confidential information in an unencrypted form over the Internet, including the emailing of such information to another County employee or to someone outside of the County.
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 device, 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.

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

a. Remote access users shall only connect to County IT infrastructure through secure encrypted channels that are authorized by agency management, e.g., Citrix, Office365, Cisco AnyConnect VPN.
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, Subscriptions and Services Procurement

In accordance with Arapahoe County Purchasing policies, all computer hardware, software, online technology services, and professional service purchases are to be done through the Information Technology Department.

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 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 Resources including email and other communication systems is the property of the 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, official 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 Hotline".

12. Related Standards and Policies

a. Social Media Policy (https://www.arapahoegov.com/DocumentCenter/View/3182/County-Social-Media-Policy---Effective-210622?bidId=)
b. Mobile Device Policy (http://inside.arapahoegov.com/DocumentCenter/View/3059/Mobile-Device-Policy---FINAL---Oct-2015?bidId=)
c. Cell Phone Policy (http://inside.arapahoegov.com/DocumentCenter/View/133/Cell-Phone-Policy?bidId=)

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.
- Broadcast messages (messages sent to large distribution lists such as department lists or building lists) are allowed but should be restricted to those instances where there is a clear business need to inform all e-mail users.
- Subscriptions to job-related internet mailing lists and newsgroups.
- 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 Communication Services or the Information Technology Service Desk. Most employee information is more appropriately distributed through another form, such as the *AC Weekly*.
- Subscriptions to non-business-related internet mailing lists.
- 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.

Revision History

Date	Revision #	Revision Type	Author
05/12/2021	AUP-1.0	E-Team presentation	David Bessen