

ITS Acceptable Use Policy: Quick Reference Guide for Employees and Vendors.

What is the Acceptable Use Policy?

The Acceptable Use Policy is a foundational policy document adopted by the Board of Supervisors that protects certain assets owned or controlled by the Napa County Information Technology Services Division.

When does the Acceptable Use Policy apply?

The Acceptable Use Policy applies to the use of all County-owned or County-controlled information assets. Information assets include, but are not limited to, hardware, software, cloud-based resources, and data.

Why is the Acceptable Use Policy important?

The Acceptable Use Policy sets out guidelines for Napa County employees and vendors for the appropriate use of County-owned or -controlled information assets. The appropriate use of information assets benefits the County by strengthening the protection of the County and its personnel and business partners from illegal or potentially damaging activities.

County employees have an ongoing obligation to ensure that these assets are secure and used appropriately. Unauthorized or improper use of County information assets may compromise the confidentiality, integrity, or availability of sensitive data, information systems, or other critical County resources.

Key Definitions

County-owned: Devices and software of which Napa County is the proprietary owner, like laptops, phones, and tablets.

County-controlled: Devices and software to which Napa County has licensed access for the purpose of conducting County business, like Microsoft Office, Granicus/Legistar, and Adobe Acrobat.

Hardware devices: A separate physical component of an information technology system or infrastructure. A hardware device may or may not be a computing device (e.g., a network hub, a webcam, a keyboard, a mouse). ([NISTIR 7695](#)).

Information assets: Information assets are owned or operated by Napa County and include but are not limited to hardware devices (e.g. laptops, cell phones), software (e.g., Microsoft Office), cloud-based resources (e.g., Sharepoint and Microsoft OneDrive), and data, and to all personnel and entities authorized to use these assets.

Software: All or part of the programs, procedures, rules, and associated documentation of an information processing system. ([NISTIR 7695](#)). Software is usually downloaded onto a system.

Cloud-based resources: A shared pool of computing resources (e.g., Microsoft OneDrive, Sharepoint, and other shared drives) characterized by on-demand, self-service access. ([NIST SP 800-145](#)).

Data: Representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means ([NIST SP 800-160v1r1](#)); *also* a representation of information, including digital and non-digital formats, from which understandable information is derived ([NIST SP 800-88r2](#)).

Quick Reference Guide	
Do	Do Not
Access only information for which you have both (1) authorized access and (2) a need-to-know, meaning that the information is necessary to the performance of their job.	Use the access privileges of another person to gain or attempt to gain unauthorized access to information.
Protect County components from unauthorized access by logging off or locking your work systems when not in use.	Circumvent or attempt to circumvent County security controls (e.g., by taking a photo of protected digital information on a personal device).
Inform the system administrator when a person's access to a particular system is no longer needed (e.g., completion of a project, transfer, graduation, retirement, resignation).	Use County information assets to store, send, or arrange to send emails or access content that includes chain letters, unauthorized mass mailings, malicious code, or pornographic, racist, or offensive material. Refrain from using the reply-all function on emails with large numbers of recipients.
Use the Sign in with Microsoft option and use your assigned County Microsoft account credentials to access or register for approved third-party applications or services.	Use personal accounts on third-party applications or services for work-related access without approval from ITS (e.g., Google Docs).
Report suspicious activity or potential threats to Napa County Information Security staff at NCIS@countyofnapa.org .	Use County information assets for personal enjoyment or an outside endeavor not related to County business in excess of incidental personal use.
Remember that your use of county information assets and their contents is not confidential or private.	Share or carelessly fail to properly conceal from discovery work-related accounts, passwords, PINs, security questions or answers, security tokens, or similar information or devices used for authentication and authorization purposes.
Get ITS approval before downloading any third-party software.	Access county information systems from personal devices unless explicitly authorized through ITS through approved remote access or mobile device solutions.
When in doubt, find out. Ask your supervisor about departmental practices or open an ITS help desk ticket for issues related to your hardware or software.	Introduce or unauthorized software, firmware, or hardware to any County information system (e.g., a personal or foreign USB or thumb drive).
	Use County information assets to engage in or solicit the violation of any law, regulation, policy, or standard issued by the federal government, the State of California, or Napa County.

What is incidental personal use?

Government Code Sec. 8314 permits incidental personal use of County resources.

At Napa County, this means:

- Incidental personal use of County information assets, like email, printer, or computer use, is restricted to County personnel only. Use by family members or others not affiliated with Napa County is prohibited.
- Incidental personal use must not result in direct costs to the County, cause legal action against, or cause embarrassment to the County.
- Incidental use must be infrequent and not interfere with the normal performance of personnel work duties.
- Storage of personal email messages, voice messages, files and documents within Napa County computer resources must be nominal.

Is there a duty to report if I notice any security concerns?

Yes. Personnel are required to report security concerns pertaining to County information asset security to their Napa County supervisor or Napa County ITS Information Security, NCIS@countyofnapa.org.

Security concerns can include suspicious activity from an external source. Concerns can also include suspected or actual activities and/or events indicating misuse or violation of the Acceptable Use Policy.

Does this policy apply to contractors?

Yes. Persons providing services to the County pursuant to a contract, vendors, or others who use the County's Information Systems while performing their duties, are subject to the provisions of this Policy.