**MEMORANDUM**
**COUNTY EXECUTIVE OFFICE**
**ADMINISTRATION**
County of Placer

TO: Board of Supervisors DATE: October 6, 2020

FROM: Todd Leopold, County Executive Officer
By: Chad Fenstermacher, Management Analyst

SUBJECT: Information Technology Acceptable Use Policy (Amended)

## ACTION REQUESTED

Adopt a Resolution approving an update to the Placer Administrative Manual for the Information Technology Acceptable Use Policy.

## BACKGROUND

This request is to recommend an update to the existing Information Technology Acceptable Use Policy previously updated by the Board of Supervisors on February 7, 2017. The purpose of Information Technology Acceptable Use Policy is it maintains as part of its information technology platform a computer network that includes hardware and software, voicemail, file servers, electronic mail (email), systems that allow access to the internet, cloud-based computing programs and processes, and other electronic pathways. These systems are provided to assist in the conduct of County business within Placer County

The recommended updates to the Information Technology Acceptable Use Policy includes:

1) Clarification for the term *Users*
2) Additional policies for authorization and accountability to identify individual, public, and generic network accounts and their uses
3) Clarification on procedures in the event of password exposure
4) Guidance on password strength and length of use
5) Clarification on procedures for disabling network accounts
6) Clarification on the actions taken for unauthorized access or circumventing protection mechanisms
7) Clarification of Department Responsibilities: vendor and licensing compliance; authorized staff permissions; procedures for media device use and reporting security issues; and security practices for patches and updates, lifecycles, sensitive data, single sign-on and backups
8) Clarification of the prohibited activities for non-County devices and remote sessions

It is also recommended with the approval of this policy the Data Network Security Standards Policy be removed from the Placer Administrative Manual and archived as the Information Technology Acceptable Use Policy incorporates any current and relevant security policies.

In addition to these updates, some areas of this policy have been reorganized for clarity.

These updates are recommended by the Placer Administrative Manual (PAM) Committee, comprised of representatives of the Auditor-Controller, County Executive Office, County Counsel, Risk Management, Human Resources, Information Technology and Facility Services.

**FISCAL IMPACT**
None

**ATTACHMENTS**
Resolution

# Before the Board of Supervisors
# County of Placer, State of California

**In the matter of:**

An update to the Placer Administrative Manual for the Information Technology Acceptable Use Policy

Resolution No.: _____

The following Resolution was duly passed by the Board of Supervisors of the County of Placer at a regular meeting held_____October 6, 2020_____, by the following vote on roll call:

Ayes:

Noes:

Absent:

Signed and approved by me after its passage.

_____
Chair, Board of Supervisors

Attest:

_____
Clerk of said Board

---

WHEREAS, the purpose of the Information Technology Acceptable Use Policy is it maintains as part of its information technology platform a computer network that includes hardware and software, voicemail, file servers, electronic mail (email), systems that allow access to the internet, cloud-based computing programs and processes, and other electronic pathways. These systems are provided to assist in the conduct of County business within Placer County;

WHEREAS, the existing Information Technology Acceptable Use Policy was previously updated by the Board of Supervisors on February 7, 2017;

WHEREAS, the recommended updates to the Information Technology Acceptable Use Policy includes various changes to clarify the policy regarding Information Technology use, access and security.

WHEREAS, these updates are recommended by the Placer Administrative Manual (PAM) Committee, comprised of representatives of the Auditor-Controller, County Executive Office, Human Resources, Administrative Services, and County Counsel. Updates are also supported by Placer Public Employees Organization (PPEO) representatives. This update does not address provisions that would affect Deputy Sheriff's Association (DSA) represented employees, which may be presented as a subsequent policy update at a future board meeting,

BE IT RESOLVED, that the Board of Supervisors, County of Placer, State of California adopts the updated Information Technology Acceptable Use Policy.

BE IT FURTHER RESOLVED, that the Data Network Security Standards Policy is rescinded and replaced by the Information Technology Acceptable Use Policy.

Exhibit A - Information Technology Acceptable Use Policy

# Information Technology Acceptable Use Policy

## (Computer, E-mail, Internet, Voicemail)

## 1.0 PURPOSE and DEFINITIONS

Placer County maintains as part of its information technology platform a computer network that includes hardware and software, voicemail, file servers, electronic mail (email), systems that allow access to the internet, cloud-based computing programs and processes, and other electronic pathways. These systems are provided to assist in the conduct of County business within Placer County.

1.1 Cloud computing – The practice of utilizing a network of remote servers hosted on the internet to store, manage, and process data.

1.2 Internet - The global system of interconnected computer networks that link billions of devices worldwide. The Internet carries an extensive range of informational resources and services, such as web pages, email, newsgroups, VoIP telephony, and peer-to-peer networks for file sharing.

1.3 Social Media - A category of internet site that is based on user participation and user-generated content including but not limited to online social networks, user generated audio sites, blogs and micro-blogs, social bookmarking sites, social news sites, photo-sharing, podcast, RSS, user generated video sites, web feeds, and wikis. This policy is not meant to address one form of social media, rather social media in general, as advances in technology will occur and new tools will emerge. Current examples of social media include Instagram, Snapchat, TikTok, NextDoor, Twitter, ~~Pintrest~~Pinterest, Facebook, Foursquare, LinkedIn, Reddit, and YouTube.

1.4 Users - This Policy applies to all employees, agents, vendors, consultants, volunteers, student interns, elected officials and any other person with authorized access to any component of the Placer County technology platform (hereinafter "User").

1.5 Web 2.0 - The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term inter-changeably with social media.

1.6 World Wide Web (WWW) - An information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the Internet.

## 2.0 POLICY

2.1 ~~2.1~~ Ownership and Control

All components of the Placer County Technology Platform, including voicemail, email messages sent and received, files and records created or placed on any County file server, and all data placed onto or accessed by the County's computer network including internet access, are and remain either the property of or under the control of Placer County and not the User.

## ~~2.4~~2.2 ~~2.2~~ Access and Privacy

Placer County, through the Department of Information Technology (IT), has access to all information technology and electronic equipment and data (computer, voicemail, email, directories, files, electronic records, and Internet and Cloud access). Placer County reserves the right to retrieve and review any voicemail, email, directory, file, record or Internet access records composed, sent, accessed by, or received on its systems.

2.2.1 Users should be aware that, even when a message or file is erased or a visit to a website is closed, it is still possible to recreate the message, file or Internet access records.

2.2.2 All communications, including text and images may be disclosed by management to third parties or law enforcement, and/or may be used by management for any other lawful purpose including discipline or vendor disputes without prior consent of the sender or receiver.

2.2.3 Users have no right to privacy as to any information or file stored on or transmitted through Placer County's computer systems including the internet and cloud, voicemail system, email or other technical resources.

## 2.3 ~~2.3~~ Authorization and Accountability

2.3.1 Each individual must have a separate log-in account and password for network use.

2.3.2 Public and generic accounts must be restricted to specific workstation(s) and assigned to workgroups for select, specific business processes approved by Leadership Committee.

## ~~2.3~~2.4 Passwords

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Placer County's resources. All users, including contractors and vendors with access to the County's systems, are responsible for the creation and protection of passwords. Users must not use the same password for Placer County accounts and personal accounts.

The reliability of passwords for maintaining confidentiality cannot be guaranteed. Always assume that someone, in addition to the intended or designated recipient, may read any and all messages and files. Any user suspecting that his/her password may have been compromised must, without delay, report the incident to IT.

2.4.1 ~~2.4~~ Passwords must never be shared or disclosed. If a password is accidentally exposed or suspected of exposure, the password should be changed immediately.

2.4.2 All passwords must be changed on a specified, periodic basis.

2.4.3 Default passwords provided by the vendor for access to applications/systems on the network must be changed to unique and secret passwords.

2.4.4 Immediately inform the Information Technology Service Desk when user accounts are no longer required or will not be used for a period of 30 days or more.

2.4.5 All accounts not used for 90 days will be automatically disabled.

## ~~2.4~~2.5 Authorized Access

~~2.4.1~~2.5.1 ~~2.4.1~~ Users may access only the messages, files, or programs that they have authorization to use and where that use, or access is actually needed to perform their work duties. Unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems or programs, voicemail messages, or other property of Placer County, or improper use of information obtained by authorized means is a violation of this Policy.

~~2.4.2~~2.5.2 ~~2.4.2~~ Access to any internet based site, including Cloud or social media site, is limited to IT approved sites and access or use may be prohibited by IT on the ground that the access poses an unreasonable risk to County network security, or the site primarily includes content that is prohibited under this Policy. Access to any other site may be prohibited at the request of a Department Head with concurrence of the County Executive Officer.

2.5.3 ~~2.5~~ Attempts to circumvent protection mechanisms and standards to gain unauthorized access will be subject to disciplinary action.

## ~~2.5~~2.6 Department Responsibility

Department Heads have the responsibility for the management of this Policy in their departments and for developing department specific policy identifying appropriate Users and appropriate use of these technology systems given the business and role of the department. Departments have the responsibility to ensure that their department or program specific web sites and social media sites meet current County issued guidelines and protocols, including record retention obligations.

2.6.1 ~~2.6~~ Vendors must comply with Placer County security standards and it is the responsibility of the department involved to monitor this compliance.

2.6.2 Security vulnerabilities and suspicious or illicit use of information technologies should be reported to your immediate supervisor or the Information Technology Service Desk.

2.6.3 Only authorized staff should maintain, move or modify County network systems and components.

2.6.4 If removable media devices are used, they must be scanned with an antivirus solution when plugged into the Placer County network.

2.6.5 Licensing requirements and copyright laws must be adhered to.

2.6.6 All department supported systems and devices must be maintained with the current security patches and updates.

2.6.7 Security lifecycle practices must be practiced in all development cycles.

2.6.8 Per the Information Security Program Charter, data sensitivity is established by the department owning the information. All sensitive or confidential data must be protected in transit and when stored.

2.6.9 Applications should employ Single Sign On technology.

2.6.10 Business critical systems and data must be backed up with periodically validated processes.

## ~~2.6~~2.7 Content Standards

Information obtained, created, sent, received or posted by any User or by the public while using a component of the Placer County Technology Platform may not include or link to content that may be unlawful or violate this or other identifiable County Policy or law. Examples of prohibited content include but are not limited to:

a. Anything that would violate the County's Policy Against Workplace Harassment, Discrimination and Retaliation.
b. Anything that would violate the County's Policy Against Workplace Violence.
c. Improper Political Activity including campaign activity.
d. Use of County resources for private gain or profit as described in California Government Code section 8314.
e. Unlawful dissemination of copyrighted or trademarked material owned by others.
f. Disclosure of Placer County's confidential or proprietary information.
g. Use of "Obscene, Indecent or Profane" content, as those three terms are described by the U.S. Federal Communications Commission in its regulations and Consumer Guidance.
h. The conduct or encouragement of illegal activity.
i. Content that constitutes a specific and eminent threat.
j. Content that violates a third-party site's reasonable and neutral terms of service.

## ~~2.7~~2.8 User Behavior

As with other work tools, authorized access and use of all components of the County's Technology Systems, including remote access to the County Network and use of County provided wireless access, is provided to employees and other authorized Users for the benefit of the County of Placer in service of its citizens, customers, vendors and suppliers. Use must be related to County business.

### ~~2.7.1~~2.8.1 Examples of Acceptable uses:

~~2.7.1.1~~2.8.1.1 Users are representing Placer County in all communications, including postings and email outside the County's email network. All communications should be made in a professional manner. The same standards, principles and guidelines that apply to Placer County

employees in the performance of assigned duties apply to User use of County technology systems.

2.8.1.2 Each User is responsible for ensuring that they use their access privileges in an effective, ethical and lawful manner.

~~2.7.1.2~~2.8.1.3 Users may access County web pages and social media sites and access their personal social media sites from work computers to share officially released County news and information, and as otherwise authorized to perform their duties.

~~2.7.2~~2.8.2 Examples of Unacceptable uses include but are not limited to:

~~2.7.2.1~~2.8.2.1 Sending, posting, saving, viewing or disseminating unlawful or offensive material, as described in the Content Standards, section ~~6~~2.7, of this Policy.

~~2.7.2.2~~2.8.2.2 Users shall not host or hold-out a website or social media page in a manner which states or suggests that the page is an officially hosted or approved Placer County entity site or department or program site.

~~2.7.2.3~~2.8.2.3 Users shall not destroy or fail to preserve electronic records in violation of the County's Records Management, Retention and Destruction Policy or the California Public Records Act.

~~2.7.2.4~~2.8.2.4 Users should not use personal sites to conduct County business.

~~2.8~~2.9 Advance Overtime Authorization Requirement

Non-exempt (hourly) employees understand that using remote access via home computer, or county assigned or personal device during off duty days or hours may create a county obligation to compensate the employee with overtime pay. Therefore, the non-exempt employee shall not access county resources during off-duty hours or days without receiving advance approval from their supervisor to do so.

~~2.9~~2.10 User Identification

Each employee and other authorized User ~~is~~are responsible for the content of all text, audio, or images that they create and send or share. All messages communicated should have the User's name attached; messages may not be transmitted using someone else's name or under an assumed name. Employees and authorized Users who wish to express personal opinions should do so on their own time and with their own system and access.

~~2.10~~2.11 ~~2.10~~ Use of Employee Photographs

Some applications, sites or functions within the Placer County Technology Platform may allow for the upload of a User photo, known as a personal icon or Avatar. Users

are only authorized to use their official County badge identification card photograph on all sites, applications and functions within the Placer County Technology Platform.

The User is authorized to copy-and-paste their official County badge identification photograph from the Workday application into other County applications, websites, and technology functions where appropriate. The use of any other photograph or image to include cartoons, political statements, clip art, etc. will be considered a violation of this policy and may be subject to discipline by the Department Head.

~~2.11~~2.12 ~~2.11~~ Prohibited Activities

To prevent computer viruses from being transmitted, to protect Placer County information and records, and to protect against inadvertent violations of section ~~6~~ 2.7 of this Policy, Users are prohibited from performing the following activities without first obtaining authorization from the IT Department. Authorization may occur individually, pursuant to a pre-approved list of allowable programs or activities, or by provision of a product approved by the IT Department to a department, User, or to the County generally. The following activities are otherwise prohibited:

~~2.11.2~~2.12.1 Do not download any software onto a County computer, network drive, or mobile communications device.

~~2.11.3~~2.12.2 Do not transfer, that is upload or download, documents, videos or information to or from an unauthorized Cloud based service or related website.

~~2.11.4~~2.12.3 Do not send email with large attachments as a Broadcast to All Employees.

2.12.4 ~~2.12~~ Do not plug non-County devices into the network.

2.12.5 Disconnect remote sessions to the network when the work is completed.

~~2.12~~2.13 Procedures and Training Implementing this Policy

Procedures, training, forms and acknowledgements implementing this Policy may be created by the Information Technology Department and authorized by the Chief Information Officer and the County Executive Officer. Any of those may be mandated for use by a User and will be considered a part of this Policy.

~~2.13~~2.14 ~~2.13~~ Violations

~~2.13.1~~2.14.1 ~~2.13.1~~ Violations of any portion of this Policy, or any guidelines, procedures or forms created to supplement this Policy may result in disciplinary action up to and including termination. Placer County management may advise appropriate law enforcement officials of any alleged illegal acts related to use of any component of the County's Technology Platform.

~~2.13.2~~2.14.2 ~~2.13.2~~ The Department of Information Technology may revoke or limit the use or access of any User for violations of this Policy. The Chief Information Officer reserves the right to deviate from this policy in emergency circumstances.