

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 1 of 9

1.0 Policy Statement

Kaiser Permanente (KP) gives employees access to electronic assets to assist them in the performance of their work duties and has controls in place to monitor for appropriate use of these electronic assets.

2.0 Purpose

Kaiser Permanente’s electronic assets are business assets and tools. The purpose of this policy is to define appropriate use of KP’s electronic assets in compliance with federal and state regulations.

3.0 Scope/Coverage

This policy applies to all employees who are employed by the following entities (collectively referred to as “Kaiser Permanente”):

- 3.1** Kaiser Foundation Health Plan, Inc. (KFHP);
- 3.2** Kaiser Foundation Hospitals (KFH);
- 3.3** KFHP/H subsidiaries;
- 3.4** The Permanente Medical Group, Inc. (TPMG); and
 - 3.4.1** This policy does not apply to physicians, podiatrists, vice presidents, or members of the TPMG Executive Staff, who are covered by separate TPMG policies.
- 3.5** Southern California Permanente Medical Group (SCPMG).
 - 3.5.1** This policy does not apply to physicians of SCPMG.

4.0 Definitions

N/A

5.0 Provisions

5.1 Appropriate Use of Electronic Assets

- 5.1.1** KP Electronic Assets should be used by employees, where needed, to perform job duties and other authorized activity relating to their job functions.
 - 5.1.1.1** Electronic assets are any and all KP electronic media and computing systems/devices, including but not limited to laptops and other portable devices, including iPads, voicemail, email, landline phones, cell phones, smartphones, tablets, mobile broadband/air cards, instant messaging (e.g.,

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 2 of 9

MS Teams, etc.), faxes, pagers, shared media (e.g., drives, SharePoint, cloud storage), and internet access. The use of Electronic Assets that are defined as Mobile Devices (such as cell phones and other handheld data and communication devices) may have additional usage requirements in accordance with applicable regional/national policies, such as TPMG and SCPMG policies regarding cell phone usage.

- 5.1.1.1.1** Electronic media are non-computing devices such as diskettes, flash memory drives, CDs, DVDs, tapes, hard disks, internal memory, memory cards, and any other interchangeable, reusable, and/or portable electronic storage media (1) on which electronic information is stored, or (2) which are used to move data among computing systems/devices. Printers, copiers, faxes, scanners, and similar devices may contain information storage units; these storage units are considered electronic media and subject to all applicable controls.
- 5.1.1.1.2** Computing systems/devices are software and/or hardware used to store, transmit, and/or monitor electronic information, including information technology equipment that connects or potentially can connect to KP networks, whether owned by KP or not. Any printers, copiers, scanners, fax machines, or other equipment used for printing, copying, scanning, transmitting, or receiving Confidential and Proprietary Information (as defined in this policy), are connected to the KP network, and which may or may not be secured by physical or technical security controls, such as locked rooms, access keys, or user ID/account codes are considered computing systems/devices.
- 5.1.1.1.3** Confidential and/or proprietary business information includes any information that is not intended to be accessible to the public; gives KP a competitive advantage in doing business; or, if disclosed to a third party or the public, could reasonably be expected to be harmful to KP members and patients.

This includes KP records or information in any form (verbal, written, or electronic) related to non-public business plans, strategies and techniques, research and development plans,

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 3 of 9

data, objectives, and unreleased, draft, or preliminary findings and conclusions (including service, marketing, member, licensing and purchase agreements), legally protectable financial information such as performance data and forecasts; customer accounts, intellectual property (e.g., inventions, discoveries, trade secrets), member rates and benefits, technical data or drawings, product and technical information about software programs and service development, audits, privileged and/or protected quality and peer review records, attorney-client privileged or attorney work product materials, other legal documents and communications, and any other records and information that are marked as confidential and/or proprietary (e.g., business concepts, strategies and plans, clinical and financial data, intellectual property, reports, and report formats). For more information, see *Data Protection, NATL.IS.021*.

Note: Confidential information does not include information about wages, hours, benefits, and other terms and conditions of employment.

- 5.1.2** Communication using KP Electronic Assets (e.g., email) must be in compliance with federal, state, and local laws, KP’s Principles of Responsibility, and KP policies.
- 5.1.3** Employees’ use of KP Assets to participate in social media (e.g., blogs, podcasts, discussion forums, and social networks) must comply with *Social Media, NATL.COMM.001*.
- 5.1.4** Employees who become aware of the misuse of Electronic Assets should notify their supervisor or an HR Representative.
- 5.1.5** Employees must refrain from using their mobile device in areas where the devices are prohibited.
 - 5.1.5.1** Hospitals and specific business units may impose stricter requirements than required by this policy.
- 5.1.6** Employees are required to comply with applicable laws related to use of Mobile Devices while driving.
 - 5.1.6.1** Mobile devices refer to smartphones, tablets and other handheld data and communication devices, including associated accessories such as mobile broadband devices (WiFi and air card). The definition of Mobile Devices specified herein may be modified to address changes in

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 4 of 9

technology. Any new features and functionality that augment or enhance Mobile Devices will be subject to this policy.

5.1.6.2 Employees charged with traffic or other violations resulting from the use of Mobile Devices while driving or in restricted or unsafe environments are solely responsible for the consequences of the violation.

5.1.7 The ability of employees to clock in using an electronic asset is limited to specific job classifications and specific regions/national functions, per *Employee Time and Attendance, NATL.HR.054*.

Non-exempt employees may not work outside their scheduled work hours without prior management approval to conduct KP business including taking phone calls, reviewing, and responding to email or voice messages, etc.

5.2 Personal Use of KP Electronic Assets

5.2.1 Personal use of KP Electronic Assets, as defined in this policy, must be incidental, limited in frequency and scope, cannot incur additional costs to KP, should comply with all KP policies, and cannot impact employee performance (see TPMG and SCPMG policies regarding cell phone usage).

5.2.1.1 Personal use is the use of KP electronic assets that is for personal reasons that do not relate to an employee’s work for KP or other issues relating to KP.

5.2.2 Employees should not send “mass” personal messages (sent to large numbers of recipients). For example, employees may not use KP’s Electronic Assets to initiate or forward chain letters, jokes, or other personal mass mailings that have no business purpose. Employees may only send authorized messages to large numbers of recipients when there is a clear business need to do so, and only as authorized by the appropriate KP manager.

5.3 Prohibited Use of KP’s Electronic Assets

5.3.1 Employees may not use KP Electronic Assets to access any Confidential and Proprietary Information, except as authorized in accordance with established KP processes and only for business or medical care reasons. Employees may not access their own medical records except in accordance with established policies and procedures (see *Obligations Regarding Confidentiality, NATL.HR.031*).

5.3.2 Employees may not use KP’s Electronic Assets in any way that may violate KP policies with respect to harassment, discrimination, retaliation, or other policies governing workplace conduct including, but not limited to, the Principles of Responsibility.

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 5 of 9

For example, employees may not use KP’s Electronic Assets to send, forward or store sexually explicit messages, cartoons, jokes, videos, or unwelcome propositions, or content that is derogatory to any individual or group of people based on such protected categories as race, religion, gender, national origin, gender identity or sexual orientation. Employees may not use KP’s Electronic Assets to access or view pornographic or sexually-oriented material, or any content relating to gambling or weapons production. Some medical staff may need to access material that deals with human sexuality as part of their jobs; this is not meant to restrict those legitimate job-related activities.

- 5.3.3** Employees may not use KP’s Electronic Assets in a manner that detracts from quality patient care, security and accuracy of medical and business records, courteous member service or the employee’s efficient performance of their duties.
- 5.3.4** Employees may not use KP’s Electronic Assets to solicit or advocate for commercial ventures, religious causes, political candidates or parties, or outside organizations (such as cosmetics sales, churches, clubs) or other similar, non-job-related solicitations. The use of KP’s Electronic Assets in this manner may jeopardize the tax-exempt status of KFHP/H and their collective subsidiaries. This provision does not apply to communications made by employees during non-working time that are protected under Section 7 of the National Labor Relations Act.
 - 5.3.4.1** Working time is time during which an employee is required or scheduled to be on duty, exclusive of break time, mealtime, or time before and after required or scheduled work.
- 5.3.5** Employees may not download or run audio, video, picture or other large data files that require significant computer storage space and may impact KP system operations unless such files are business-related.
- 5.3.6** Employees may not use voicemail to make unauthorized broadcast messages.
- 5.3.7** Unless expressly authorized by a policy and procedure approved by KP, employees may not use KP’s Electronic Assets to send, transmit, or otherwise disseminate or take away Confidential or Proprietary Information (as defined in this policy).
- 5.3.8** Employees may not make audio, digital, live-streaming, or video recordings on KP premises, or of KP personnel, patients or their family members, with personal or KP Electronic Assets, without the consent and authorization of all who are being recorded. Consent is implied or is not required in certain limited situations, such as KP security system recordings and KP-authorized events (e.g., Town Hall events, executive leadership forums, KP Compliance awareness fairs, retirement award celebrations, KP Thrive events). See *Video Recording for Quality*

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 6 of 9

Improvement NATL.HPHQ.012 for the requirements on video recording patients, members, and staff. Employees may not download unauthorized software to any KP Computing Systems.

- 5.3.9** Employees may not use KP electronic assets or non-KP electronic devices in any manner that negatively impacts the operation of KP’s network or computing systems/devices, or that presents risks to the confidentiality, integrity, or availability of KP medical and business information.

5.4 Issuing Electronic Assets

- 5.4.1** KP managers may only issue employees laptop computers, cellular telephones, pagers or other portable electronic equipment when those employees need the portable equipment to assist them in performing their KP job duties, and when any other applicable requirements to receive Electronic Assets have been met.
- 5.4.2** Employees approved to have a mobile device will purchase the device and service through established KP Preferred Service Providers utilizing KP procurement policies and procedures and the authorized procurement web portal. Budget for the operation of a mobile device is the responsibility of each Department Manager.
- 5.4.3** KP employees who receive or use KP Electronic Assets are responsible for returning the Electronic Assets when they no longer have a business need to use them, such as upon transfer or termination.
- 5.4.4** Managers are responsible for collecting KP Electronic Assets from employees and for terminating or transferring mobile phone service for employees who no longer have a business need to use them, such as upon transfer or termination.
- 5.4.5** KP managers may not give away KP Electronic Assets to employees or charities without following *Capital Asset Obsolescence, Disposal, Donation, Sale and Trade-In, NATL.FIN.ACCT.053* and *In-kind Contributions, NATL.CB.207*.

5.5 Privacy Considerations

- 5.5.1** All information about KP Electronic Asset usage, including but not limited to any email messages, instant messages, text messages, voicemail messages, internet/webpage access, computer files and data generated from, sent by, visited using, or saved on KP Electronic Assets, is accessible to KP and may be subject to review, if needed.
- 5.5.2** Electronic assets provided by KP are business devices. The device and all data on the devices are the property of KP.
- 5.5.3** KP may access and review any records of KP Electronic Asset usage without the permission of employees unless such access or review is otherwise restricted by law. Accordingly, employees should not have an expectation of privacy regarding usage of KP Electronic Assets and

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 7 of 9

should not use KP Electronic Assets for communications or activities that they wish to keep confidential.

5.5.4 Backup copies of email messages, instant messages, text messages, voicemail messages and computer files may also be saved or maintained by KP even after the user has deleted them. In accordance with authorized procedures, KP management and IT staff have the ability to override employee passwords as needed.

5.6 Maintaining Security and Confidentiality

5.6.1 Employees must maintain the confidentiality of their work when it includes any Confidential or Proprietary Information (as defined in this policy). Employees must limit distribution of Confidential and Proprietary Information to persons who are authorized to receive the information and have a business or medical need to know.

5.6.2 Employees are responsible for maintaining security of KP Electronic Assets and confidentiality of KP data, which includes the following:

5.6.2.1 Taking precautions to prevent unauthorized users from accessing KP’s Electronic Assets, including encryption on all portable devices that may contain Confidential and Proprietary Information;

5.6.2.2 Not disclosing their passwords to any person and not obtaining, possessing, or using anyone else’s logon ID or other access code or password;

5.6.2.3 Taking precautions so that their use of KP information and other Electronic Assets, particularly in the context of mobile and home computing systems/devices, does not compromise the security of KP’s computer network;

5.6.2.4 Taking precautions to prevent the loss or theft of KP Electronic Assets. This includes, but is not limited to, maintaining personal custody when traveling (e.g., making sure laptops are not left unattended in vehicles);

5.6.2.5 Complying with applicable state and federal laws and regulations in accessing, maintaining, and disclosing Confidential and Proprietary Information;

5.6.2.6 Following KP policies for the handling, distribution, and maintenance of electronic information (e.g., complying with the requirements for storage and protection of PHI and other information per *Data Protection, NATL .IS.021*); and

5.6.2.7 Following any applicable encryption procedures when transmitting Confidential and Proprietary Information and using an appropriate mode of transmission of highly sensitive material.

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 8 of 9

5.7 Loss, Theft, or Damage

- 5.7.1 Employees must immediately report lost, stolen, or damaged KP Electronic Assets to their manager, IT Security, and the service provider (for mobile devices).
- 5.7.2 If fraudulent use is known or suspected, this should be reported to the Ethics and Compliance.

5.8 Compliance Expectations

- 5.8.1 KP reserves the right to suspend and/or revoke some or all forms of Electronic Asset access for employees who misuse assets or otherwise violate this policy.
- 5.8.2 Employees who misuse KP Electronic Assets in violation of this policy will be subject to appropriate corrective/disciplinary action.
- 5.8.3 KP also may refer incidents of serious misuse of KP Electronic Assets to law enforcement or other licensing or regulatory agencies as appropriate.

6.0 Resources

6.1 Attachments

- 6.1.1 Intent of HR Policies

6.2 Kaiser Permanente Policies

- 6.2.1 [Acceptable Use of KP Information Systems and Assets](#), NATL.IS.002
- 6.2.2 [Capital Asset Obsolescence, Disposal, Donation, Sale, and Trade-In](#), NATL.FIN.ACCT.053
- 6.2.3 [Commitment to a Harassment-Free Work Environment](#), NATL.HR.005
- 6.2.4 [Corrective / Disciplinary Action](#), NATL.HR.014
- 6.2.5 [Data Protection](#), NATL.IS.021
- 6.2.6 [Employee Time and Attendance](#), NATL.HR.054
- 6.2.7 [Financial Communications](#), NATL.FIN.ACCT.099
- 6.2.8 [In-Kind Contributions](#), NATL.CB.207
- 6.2.9 [Use of Health Plan or Hospitals Facilities and Assets by Others - Compliance With Tax Exempt Status Regulations](#), NATL.HR.031
- 6.2.10 [Code of Ethical Conduct - Kaiser Permanente's Principles of Responsibility](#), POR
- 6.2.11 [Processing Employee Terminations](#), NATL.HR.013

POLICY TITLE Electronic Asset Usage	POLICY NUMBER NATL.HR.025
ACCOUNTABLE DEPARTMENT Human Resources	EFFECTIVE DATE 06/20/2024
DOCUMENT OWNER Chair, National HR Policy Roundtable	PAGE 9 of 9

- 6.2.12 [Sanctions by KP Against Workforce Members for Failure to Comply, NATL.EC.PRIV.019](#)
- 6.2.13 [Secure Electronic Communication, NATL.IS.010](#)
- 6.2.14 [Social Media, NATL.COMM.001](#)
- 6.2.15 [Use of Health Plan or Hospitals Facilities and Assets by Others - Compliance With Tax Exempt Status Regulations, NATL.FIN.ACCT.116](#)
- 6.2.16 [Uses and Disclosures of PHI and Minimum Necessary, NATL.EC.PRIV.014](#)

7.0 Approval

This policy was digitally approved by the following representative of Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and their subsidiaries.

Approver:

Frank Hurtarte
SVP HR Consulting

Approval Date: 05/20/2024