

1. Overview

Pacifica's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Pacifica/KPFK's established culture of openness, trust and integrity. Pacifica is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of Pacifica/KPFK. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Pacifica/KPFK employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of technical, computer and/or broadcast equipment at Pacifica/KPFK. These rules are in place to protect the employee and Pacifica/KPFK. Inappropriate use exposes Pacifica/KPFK to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Pacifica/KPFK business or interact with internal networks and business systems, whether owned or leased by Pacifica/KPFK, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Pacifica/KPFK and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Pacifica/KPFK policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Pacifica/KPFK, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Pacifica/KPFK.

4. Policy

4.1 General Use and Ownership

- 4.1.1 Pacifica/KPFK proprietary information stored on electronic and computing devices whether owned or leased by Pacifica/KPFK, the employee or a third party, remains the sole property of Pacifica/KPFK. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard*.
- 4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Pacifica/KPFK proprietary information.
- 4.1.3 You may access, use or share Pacifica/KPFK proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- 4.1.5 For security and network maintenance purposes, authorized individuals within Pacifica/KPFK may monitor equipment, systems and network traffic at any time, per Pacifica/KPFK's *Audit Policy*.
- 4.1.6 Pacifica/KPFK reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

- 4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.
- 4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- 4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- 4.2.4 Postings by employees from a Pacifica/KPFK email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Pacifica/KPFK, unless posting is in the course of business duties.
- 4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of 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 Pacifica/KPFK authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Pacifica/KPFK-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or 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 Pacifica/KPFK.
2. 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 Pacifica/KPFK or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Pacifica/KPFK business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Pacifica/KPFK computing asset 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.

8. Making fraudulent offers of products, items, or services originating from any Pacifica/KPFK account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting 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, unless these duties are within the scope of regular duties. 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.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Pacifica/KPFK is made.
12. 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.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the Pacifica/KPFK network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Pacifica/KPFK employees to parties outside Pacifica/KPFK.

4.3.2 Blogging and Social Media

1. Blogging by employees, whether using Pacifica/KPFK's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Pacifica/KPFK's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Pacifica/KPFK's policy, is not detrimental to Pacifica/KPFK's best interests, and does not interfere with an employee's regular work duties. Blogging from Pacifica/KPFK's systems is also subject to monitoring.
2. Pacifica/KPFK's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Pacifica/KPFK confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Pacifica/KPFK and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Pacifica/KPFK's *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to Pacifica/KPFK when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Pacifica/KPFK. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Pacifica/KPFK's trademarks, logos and any other Pacifica/KPFK intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

The Pacifica/KPFK team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Pacifica/KPFK team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy