

[Browse](#)[Search](#)[Support](#) [English](#)[Corporate](#) ▾

Workplace Searches and Privacy

In order to protect Apple confidential and sensitive information and maintain the security and integrity of our networks and equipment, any use of Apple property, as well as use of your personal devices for Apple business or for accessing Apple networks, is subject to this policy.

Use of Apple systems and data

All Apple facilities, furnishings, supplies, equipment, networks, and electronic systems (such as internet and intranet access, voicemail, email, instant messaging, and collaboration tools) are company property and are provided to conduct Apple business. Personal use is permitted as long as such use is reasonable and doesn't interfere with normal business activities. It must also not affect your performance, violate Apple policies and practices, or applicable local laws.

Generally, you should use Apple equipment to conduct Apple business. If you use your personal property to conduct Apple business (such as computers, data storage devices, mobile devices, and so on), or to access Apple networks, you must act in accordance with Apple policies. In addition, your property may be subject to search and the Apple-related content may be removed.

Workplace searches

Only in cases where allowed under local law, Apple may:

- Access, search, monitor, archive, and delete Apple data stored on all of its property, as well as non-Apple property, if used for Apple business or if used for accessing Apple data, servers, or networks. This includes all data and messages sent, accessed, viewed, or stored (including those from iCloud, Messages, or other personal accounts) using Apple equipment, networks, or systems.
- Conduct physical, video, or electronic surveillance, search your workspace such as file cabinets, desks, and offices (even if locked), review phone records, or search any non-Apple property (such as backpacks, purses) on company premises.

This means that you have no expectation of privacy when using your or someone else's personal devices for Apple business, when using Apple systems or networks, or when on Apple premises.

The search or removal of Apple-related content on a device will be determined on a case-by-case basis when there is a business need and subject to local approval processes. Refusing to permit a search or removal of Apple-related content may result in disciplinary action up to and including termination of employment.

If you visit the premises of current or potential customers, clients, suppliers, or vendors, you may be subject to their respective search policies and procedures. Before providing access to Apple materials, contact your manager or [Global Security](#).

Information disclosure

If information discovered during any search indicates possible unlawful behavior, Apple may disclose that information to law enforcement officials without notice.

Additional resources

[Business Conduct and Compliance](#)

[Global Security](#)

[Harassment](#)

[Information Security Policies](#)

[Solicitation and Distribution](#)

[Workplace Violence](#)

[Misconduct and Discipline](#)

[Personally Identifiable Information](#)

[Employee Use of Electronic Systems and Communications](#)

Was this page helpful?

Yes

No

41 people found this page helpful.

Need additional support? We're here to help.