



Device preservation checklist

For employee departures and retaliation matters

Preserve first, examine later. Most evidence in these disputes is lost in the first few days, when IT resets the laptop or phone and hands it to someone else.

General guidance, not legal advice. Preservation duties depend on each matter and should be set by counsel.

Before the separation meeting

- ☐ List every device assigned, with asset tags or serials: laptop, phone, tablet, external drives.
- ☐ List the accounts used: email, Teams or Slack, cloud storage, CRM, and any personal phone in device management.
- ☐ Tell IT in writing: no wiping, reimaging, or reissuing until counsel releases them.
- ☐ Pause automatic deletion and retention rules on mail, chat, and cloud storage.
- ☐ Decide who collects the devices and where they get locked up.
- ☐ If a dispute is reasonably expected, have counsel issue a litigation hold.

What not to do

- ✗ Reset, reimage, or reissue the device, even if a new hire needs it.
- ✗ Let a manager or IT "take a look." Browsing changes dates and metadata, and makes that person a witness.
- ✗ Drag files to a thumb drive as a backup. That copy isn't a forensic image.
- ✗ Rely on screenshots as the only record of messages.
- ✗ Delete the account or let its license lapse. Some platforms purge data on a timer.
- ✗ Log into personal accounts or devices without consent and counsel's direction.

On the day of separation

- ☐ Collect each device as it is. If it's off, leave it off. If it's on, don't browse it.
- ☐ Put phones in airplane mode and keep them charged to block a remote wipe.
- ☐ Ask for passcodes and write them down. Ask whether personal devices or accounts were used for work.
- ☐ Suspend logins. Don't delete accounts or remove licenses.
- ☐ Bag and label each device. Start a chain-of-custody log: who took it, when, where it went, and its condition.
- ☐ Store the devices in a locked space with a sign-out sheet.

When to bring in an examiner

Call before anyone reviews the device.

- The employee joined a competitor or started a business, especially under a non-compete.
- There are signs of large downloads, USB use, personal cloud uploads, or forwarding to personal email.
- The claim turns on texts, screenshots, or recordings that may be challenged as edited or AI-generated.
- A device came back late, reset, or missing data.
- The other side produced its own forensic report.