

Screen recording privacy checklist

A practical checklist for product demos, tutorials, support videos, training clips and internal walkthroughs. The goal is to keep sensitive data out of the source recording rather than depend on blur afterward.

VISIBLE PIXELS	SPOKEN AUDIO	INTERACTION DATA	DERIVED CONTENT
Prevent exposure at the source.		Retake clean footage when practical. Review the rendered file, its captions and its destination before publishing.	

Before recording

8 checks

Prepare a clean environment before any private detail can enter pixels, audio or menus.

- ☐ Use a dedicated demo account with synthetic names, messages, analytics and payment details.
- ☐ Enable Do Not Disturb or a Focus mode on the Mac and any mirrored device.
- ☐ Close email, chat, calendar, password managers, terminals and unrelated browser profiles.
- ☐ Remove private filenames from the desktop, Downloads and recent-file menus.
- ☐ Inspect open-tab titles, bookmarks, browser profiles and autofill suggestions.
- ☐ Replace the clipboard with a neutral value before demonstrating paste.
- ☐ Confirm the exact screen or window that will be captured.
- ☐ Make and inspect a ten-second test recording.

During the take

5 checks

Stay on the rehearsed path. If exposure occurs, stop and prefer a clean retake.

- ☐ Follow a rehearsed path through inspected demo data.
- ☐ Avoid untested search boxes, file pickers, address fields and recent-item menus.
- ☐ Stop and note the time immediately if private information appears.
- ☐ Retake a clean section when practical instead of depending on a moving mask.
- ☐ Remember that anything visible in pixels can enter the video, even when typed keystrokes are not retained separately.

Review what the recording created

Privacy review continues after capture. Inspect the exported file, transcription, prompts, metadata and publishing destination as separate surfaces.

Before publishing

7 checks

Review the complete rendered artifact through sight, sound, captions and metadata.

- ☐ Watch the complete rendered file at normal speed with sound.
- ☐ Watch it again without sound and inspect transitions, menus and notification areas.
- ☐ Listen without looking for names or private details in narration or system audio.
- ☐ Inspect several frames before and after every blur or mask.
- ☐ Review captions separately for details surfaced by transcription.
- ☐ Check the export filename and metadata for customer, project or employee names.
- ☐ Confirm that the sharing destination and access settings match the audience.

When an AI agent is connected

4 checks

The editor's local boundary and the assistant provider's data controls are separate decisions.

- ☐ Keep prompts focused on editorial intent; do not paste secrets into them.
- ☐ Review the agent provider's data controls separately from the editor's local processing boundary.
- ☐ Inspect each timeline change and use undo when a result is incorrect.
- ☐ Complete the same final rendered-file review used for a manual edit.

Incident response

5 checks

If private data escapes, stop distribution and follow the organization's established process.

- ☐ Stop distribution if private data is discovered after publication.
- ☐ Remove or restrict the exposed copy at every destination you control.
- ☐ Preserve the affected file and timeline information if your security process requires investigation.
- ☐ Follow the organization's notification, legal and security procedures.
- ☐ Replace the source with a clean retake or a fully verified correction.

Operational template

This checklist is not legal or compliance advice. Copy and adapt it without attribution. Link to the maintained guide when readers should receive future corrections and product-specific privacy details.