

Data management and storage plan

A practical worksheet for institutional storage, separate permissions/key/data folders, access, retention, and disclosure review.

Original teaching templates, not official Sacramento State forms or approved protocols. Replace every bracketed prompt, remove drafting notes, use current university forms where required, and obtain the applicable institutional determination before recruitment or research. These are not ready-to-sign documents.

Drafting notes authority and storage checks

This is an original planning worksheet, not an institutional storage authorization. Public Sacramento State IRT guidance recommends SacFiles Secure for sharing Level 1 and Level 2 data. Local historical Cayuse material mentions institutional OneDrive/U: drive. Resolve the actual data classification, service, account, access, and current institutional instructions before naming any system in consent.

Do not copy a blanket retention period from another study. Confirm the required period and starting event for each record type, including any data-owner agreement, and institutional custody after graduation.

1 Inventory and privacy description

Study title/version: [title/date]. Data owner and responsible faculty custodian: [roles]. Institutional classification and confirmation: [classification, decision source, and date].

For each item, list what is collected, whether a person can be identified, and why it is necessary: [contact/eligibility records]; [consent/parent permission/assent]; [code key]; [survey or score data]; [notes/transcripts]; [audio]; [analysis files]. Remove unnecessary fields before collection.

Privacy description: [anonymous only if no identifying information or retained link exists; coded/confidential while linkable; de-identified for a specified recipient after a documented disclosure-risk review]. Check free text, voices, timing, rare characteristics, indirect identifiers, and combinations-not just names.

2 Collection and transfer

For each collection method, state the device/service, collector, temporary location, transfer channel, transfer deadline/event, verification, and removal of temporary copies: [details].

Qualtrics: [institutional account; distribution method; consent branching; identifier/metadata settings; tested incomplete-response handling; export permissions]. Paper: [private return; sealed transport; locked custody; double-checking data entry]. Audio: [separate permission; authorized encrypted capture; cloud sync controls; restricted transfer; authorized transcription; deletion event].

External AI/transcription/cloud services: [none, or the exact approved service, authorization, disclosure, and data safeguards]. Education records: [authorized custodian, variables, disclosure basis, and transfer agreement before access].

3 Storage and real access permissions

Confirmed university-authorized workspace: [service, institutional account/owner, restricted location, and verification]. Folder names are organizational aids; set and test actual permissions and inherited sharing. Do not rely on a folder name as a security control.

- Participants-Key: [contact/code linkage; custodian only; who cannot access it].
- Permissions: [consent/parent permission/assent; separate from responses; approved users].
- Questionnaires-or-Scores: [coded responses; permitted analyst access].
- Audio: [only if selected; restricted interviewer/custodian access].
- Transcripts-or-Notes: [coded records with unnecessary identifying details removed; approved users].
- Analysis-Release: [disclosure-reviewed analysis copy; what linkage remains, if any].
- Paper originals: [locked cabinet/room, key holder, authorized transport, and destruction method].
- Teacher/supervisor access: [independent custodian and exact event after which any approved cleaned data may be released].

4 Withdrawal retention and destruction

Withdrawal request route: [contact and method]. Request deadline or event: [specific point]. Who locates and removes records: [custodian]. When the key is removed: [event]. What can no longer be located after that: [data]. What must still be retained: [required records and basis].

Complete one schedule for each data type: [type] - [retention period] from [trigger] - [authorized custodian] - [destruction method]. Resolve conflicts before collection rather than choosing the shortest or longest period without authority.

Address downloaded exports, recordings, device copies, working files, backups, recycle bins, and version history: [what can be deleted, by whom, and what managed-system limits apply]. After graduation or account changes: [faculty/institutional custody and continuity arrangement].

5 Analysis sharing and final check

Analysis access: [roles and permitted files]. Public results: [aggregates, suppression/generalization of small groups, quotation editing/permissions, and contextual disclosure review]. Future research reuse or sharing: [actual plan matching every consent document]. Security concern response: [institutional reporting route and immediate containment steps].

Before collection, test an actual example export and every role's access. Compare the data plan against Cayuse, recruitment, consent/permission, assent, and instruments. Do not promise anonymous collection, deletion, confidentiality, or institutional hosting that the actual workflow cannot deliver.

Official guidance to check before use

[Sacramento State Human Subjects Research](#)

Official starting point for submission guidance and current institutional templates.

[Sacramento State Research Protocol Guidance - sign-in required](#)

Current consent forms and protocol guidance. Authenticated contents were not verified in this review.

[Sacramento State Secure Data Storage & Sharing](#)

Public IRT recommendation for SacFiles Secure when sharing Level 1 and Level 2 data; confirm study-specific arrangements.

[US Department of Education - Privacy and Data Sharing](#)

Education-record access needs an applicable disclosure basis; site permission alone is insufficient.