



Authorship & Metadata: Practical Protocols

Purpose: Practical guidance to record authorship, dates, purpose and change history for survivor-created records using recognised standards and simple workflows.

A. Minimum Metadata (Recommended "MUST" Fields)

These are the minimum details to record when a document/record is first created:

1. **Author identity** — Name, role (e.g., creator, co-creator, facilitator), and preferred display name.
2. **Creation date/time** — ISO 8601 where possible (YYYY-MM-DD). 📅 Date
3. **Purpose / Intended use** — Plain-language sentence (e.g., "personal journal for therapy" / "complaint draft").
4. **Consent status & permissions** — Who may view, share or use; date of consent and scope (workshop, public, training).
5. **Version number** — e.g., v1.0, v1.1 and short edit note.
6. **Edit history / change log** — timestamped entries recording who changed what and why.
7. **Authorship statement** — Short text describing intent, cultural context or ownership notes.
8. **Access level & retention policy** — Open / Restricted / Private, and how long retained.
9. **Accessibility outputs** — List of accessible versions produced (Easy-Read, Auslan clip, AAC export).
10. **Contact for reuse / permissions** — Email or role of person to contact about reuse. 👤 Person
11. **Audit trail reference** — Link or reference to the audit log or provenance record (could be an internal ID).
12. **Ethics & review note** — Short indicator: ethics reviewed (Y/N), review date, reviewer.

Why these matter: They preserve authorship, make consent explicit, and allow later export or legal/ethical review. (See Securing Authorship materials.)

B. Mapping to Recognised Standards (Quick Table)

Below is a table mapping the minimum metadata fields to common recognised metadata standards.

Field	Dublin Core	Schema.org	W3C PROV	PREMIS / Preservation
Author identity	dc:creator ✓	author ✓	prov:agent ✓	agent role
Creation date	dc:date ✓	dateCreated ✓	prov:generatedAtTime ✓	event/time
Purpose	dc:description ✓	description ✓	prov:activity —	preservation note
Consent status	(no direct field)	schema:conditionsOfAccess (partial)	add prov:wasAssociatedWith with role	custom metadata
Version / edits	dc:relation	schema:version	prov:wasRevisionOf ✓	PREMIS event
Accessibility outputs	(custom)	schema:encoding	link provenance	custom
Audit trail / provenance	(limited)	(limited)	prov: model is best fit ✓	PREMIS for long-term

- Use Dublin Core / Schema.org for simple web-facing metadata (search engines and basic discovery).
- Use W3C PROV for formal machine-readable provenance and audit trail when you need tamper-evidence.
- Use PREMIS for preservation workflows when long-term archival integrity is required.
- For lightweight JSON implementations, use JSON-LD + Schema.org and extend with PROV-JSON for provenance fields. (Do not publish raw sensitive fields in open Schema.org markup — mark access controlled items as such.)

C. Recommended Simple Technical Pattern

- Record metadata inside the file (where possible): e.g., Office document properties, PDF XMP metadata, or JSON-LD sidecar.
- Store a linked provenance record: for each artefact create an immutable provenance entry (timestamped) in your audit log (may be a ledger, DB or file).
- Export bundles: when exporting a record include the artefact + metadata.json + accessible outputs + consent record + provenance log. [📄 File](#)

D. Workflows (Step-by-Step)

Workflow A — Create a New Record (for a Participant)

1. Facilitator opens session record tool / template.
2. Create new artefact entry; capture MINIMUM metadata fields (author role, date, purpose, consent).
3. Save a draft file with filename pattern: YYYYMMDD_authorrole_shorttitle_v1.pdf.
4. Store file in secure folder at 📍 Place and write a provenance entry: user, action=create, timestamp.
5. If participant chooses shareable, capture explicit consent text and sign with a simple confirmation (digital signature or logged email).
6. Produce accessible output as requested (Easy-Read / Auslan / AAC export) and link in metadata.

Workflow B — Update a Record

1. Open existing artefact. Create new version: increment version.
2. Add change note to edit history: who edited, date, reason.
3. Save new file, update provenance with wasRevisionOf pointer.
4. If change affects consent (e.g., new intended public use), re-request participant's consent and log result.

Workflow C — Export / Hand-over

1. Prepare export bundle: artefact file, metadata.json, accessible outputs, provenance log, consent file. 📁 File
2. Redact or anonymise if export destination is public. Log anonymisation steps in provenance.
3. Provide simple readme describing access level and permitted uses.