



SOCIAL VALUE 360 LTD

Data Retention Policy

2026 to 2027 | Version 1.3

Policy owner: Roy Ramrutton, Privacy Lead

Prepared: 23 September 2026

Approved by: Roy Ramrutton, Responsible Director, SOCIAL VALUE 360 LTD

Approval and effective date: 23 September 2026

Next review: 23 September 2027 or earlier if required

Purpose and scope

Social Value 360 keeps records for clear purposes and disposes of them securely when they are no longer needed. This policy covers paper and electronic records, email, messages, photographs, recordings, cloud systems, backups and records held by processors. It applies to participant, safeguarding, personnel, financial and organisational information.

The UK GDPR does not set one retention period for every record. The schedule below sets organisational defaults, identifies particular legal requirements and requires case-specific review for sensitive records. A default is not permission to collect unnecessary information or keep all records for the longest period.

Responsibility

Privacy Lead: Roy Ramrutton | roy@socialvalue360.co.uk | 07789 993621. The Responsible Director approves the schedule and any justified exceptions. Record owners apply it to their systems. The safeguarding lead authorises safeguarding retention decisions with the privacy lead and specialist advice where needed. IT providers implement approved deletion and backup arrangements.

Before using a new programme or system, its owner records what is kept, why, the lawful basis, location, access restrictions, trigger date, retention period and disposal method. Confirm any commissioner or awarding-body conditions and tell participants about material programme-specific periods.

Applying the schedule

A period runs from the event stated in the schedule, not from an arbitrary file creation or migration date. Retain the minimum evidence needed for a longer legal, financial or safeguarding purpose; remove unrelated working copies sooner. Emails and messages follow their subject matter, rather than a blanket mailbox period.

The schedule is reviewed annually. Owners check disposal dates at least quarterly. At expiry, delete or irreversibly anonymise records unless a documented lawful reason requires continued retention. Record the reason, approving person and next review date. Do not retain records indefinitely because they may be useful.

Preservation and safeguarding

Suspend disposal when records are relevant to an actual or reasonably anticipated claim, investigation, safeguarding review, information request, regulatory instruction or preservation notice.

The privacy lead issues a written hold identifying the records, systems and owners. The Director releases the hold only after checking the continuing need and any external instruction.

The Independent Inquiry into Child Sexual Abuse published its final report in 2022. Existing preservation notices and other legal duties must still be checked individually; the end of an inquiry is not automatic permission to destroy records.

Safeguarding records are separated from routine participant records and have restricted access. Retention may need to extend beyond ordinary periods because of delayed disclosure, ongoing risk, serious injury or legal advice. Any extension must be reasoned, proportionate and reviewed. Do not destroy child sexual abuse records solely because a routine date has arrived without a safeguarding and legal review.

Retention schedule

Record category	Period and trigger	Basis and qualification
Enquiries not leading to participation	12 months after last meaningful contact	Organisational default; remove sooner if unnecessary.
Routine participant, referral and attendance records	Programme end plus 2 years	Default for delivery and follow-up. Separate essential funding, incident and safeguarding evidence.
Contracts and essential commissioning or funding evidence	6 years after contract or programme closure	Default for audit and claims. Check actual funder terms and any deed or statutory requirement; do not retain the full participant file automatically.
Child safeguarding records	Until age 25, then formal review	Organisational default, not a universal statutory rule. Safeguarding lead reviews ongoing risk, sexual abuse records, holds and local requirements before disposal.
Adult safeguarding records	6 years after case closure, then review	Organisational default. Extend where justified by ongoing risk, capacity, serious harm, proceedings or preservation requirements.
Allegations against staff involving children	Until normal pension age or 10 years from allegation, whichever is later	KCSIE benchmark where applicable or adopted. False or malicious allegations are removed from the personnel file unless the individual consents to retention; check lawful holds and separately necessary safeguarding evidence.
Low-level concerns about staff	At least until engagement ends, then review	Default review at departure. Retain longer only for a documented safeguarding, employment or legal purpose; patterns meeting the harm threshold follow the allegation rule.
Routine complaints and data protection complaints	6 years after closure	Organisational default. Safeguarding elements follow the safeguarding schedule. Remove unnecessary duplicates earlier.
Data breaches and rights request decision records	6 years after closure	Accountability default; retain decisions and necessary evidence rather than full copies of disclosed datasets.
Unsuccessful recruitment	6 months after decision	Default. A separate optional talent pool requires its own notice, basis and expiry.

Record category	Period and trigger	Basis and qualification
Personnel, contract and essential training records	6 years after engagement ends	Default for relevant evidence. Separate safeguarding, pensions, health surveillance and right-to-work records.
Right-to-work evidence	Employment plus 2 years	Home Office requirement for ordinary right-to-work checks; check additional sponsorship duties where relevant.
DBS certificate copies	Only as long as needed, normally no more than 6 months	Keep a limited check record and recruitment decision where necessary; restrict certificate access.
Payroll, tax and accounting records	6 years after relevant financial or tax year	Organisational default, subject to specific statutory requirements and justified longer records. Pension records require the scheme-specific retention assessment.
Adult accident records	At least 3 years after the last entry or applicable incident record date	Check the applicable accident-reporting law, insurance and any legal hold. Occupational exposure records may have much longer statutory periods.
Accident records involving children	Until age 21, then review	Default reflecting potential claims; safeguarding and serious injury records may require longer. Record the reason.
Health and safety assessments and activity plans	Superseded or activity ended plus 3 years	Default; retain relevant evidence longer if linked to an incident or claim.
Emergency contact and current medical support information	While required for current participation or engagement	Review at least annually and remove obsolete working copies promptly; preserve only necessary incident or case evidence.
Publicity photographs and testimonials	Until permission expires or is withdrawn; annual review	Remove from future use and channels under our control where appropriate. Keep minimal permission evidence for 6 years after last use as a default.
Approved session recordings	Normally 30 days after the stated purpose is fulfilled	Only if recording is approved. Set a specific deletion date before recording; incident evidence follows its relevant schedule.
CCTV if introduced	Normally no more than 30 days	Proposed maximum default, subject to a necessity assessment. Preserve relevant incident extracts separately; no statutory universal 30-day rule.
Routine security logs and visitor records	Normally 90 days	Proposed operational default; document any longer risk-based requirement. Incident evidence follows the incident schedule.
Policies, privacy notices and approval records	Superseded plus 6 years	Default; retain selected non-personal organisational history if justified. Company minutes and statutory registers follow their specific legal requirements.
Routine correspondence and duplicate working copies	Delete once purpose ends or authoritative record is filed	No blanket rule to keep every email. Apply the subject-specific schedule to substantive records.

Disposal and transfers

Before disposal, confirm that the correct period has expired, no hold applies, the record is not the sole evidence needed elsewhere and deletion is authorised. Shred confidential paper or use a vetted confidential-waste provider. Securely erase electronic media or destroy it through an approved provider before reuse or disposal.

Delete from live storage, shared drives, downloads and processor systems, including recycle bins where supported. Backups must expire on a defined cycle; a proposed default is no more than 90 days unless the approved system plan justifies longer. Until expiry, deleted information in backups must be inaccessible for ordinary use. If restored, reapply deletions and holds.

When records are transferred to another provider, verify the recipient, lawful purpose and secure method, obtain receipt and decide whether Social Value 360 must retain a minimal copy or transfer record. Do not retain a complete duplicate automatically. A change in service provider does not remove our own legal obligations.

Disposal and exception registers

The disposal log records record category, date range, unique reference, volume, authority, method, disposal date and person or contractor completing it. Do not recreate the deleted personal information in the log. Keep the log for six years as an accountability default.

An exception or hold log records reason, scope, owner, approval date and review or release date. The privacy lead reports overdue disposal and unresolved exceptions to the Director. Staff receive induction and updates and must report accidental deletion or unauthorised retention under the Data Breach Policy.

Procedure for restricting processing

This procedure applies to instructions from an organisation for which we process personal data and to requests from individuals to limit use of their personal data. Restriction means retaining identified information under controls that prevent unauthorised further use. It is not the same as deletion, a routine retention hold or ordinary access permissions. Do not delete affected records as a shortcut to implementing a restriction.

Step 1 Receive and record the request

Any member of staff may receive a request verbally or in writing; no special form or legal wording is required. Pass it immediately to Roy Ramrutton, roy@socialvalue360.co.uk, 07789 993621, who is the Privacy Lead. Roy arranges competent temporary responsibility during planned absences so requests are acted on within the required timescales. Log receipt time, requester, safe contact, relevant participant or record reference, requested scope and reasons, controller, assigned owner and response deadline. Verify identity or the authority of a controller instruction proportionately using a known contact route; request only information necessary for verification.

For controller instructions, acknowledge promptly, normally within one working day, and implement without undue delay within any shorter contractual or specified deadline. Immediately flag urgency, imminent disclosure or deletion, and any inability to meet the required scope or timing. Do not wait for an acknowledgement target before taking protective action. Verify unclear instructions promptly and use an authorised temporary safeguard to prevent the identified risky use while clarification is obtained.

Step 2 Confirm responsibility and scope

Where Social Value 360 acts as processor for another organisation, promptly forward any individual's request concerning data processed on behalf of another controller to the controller through the agreed secure route and assist its response. Record the controller's instructions. Do not independently refuse the request, decide its legal merits, lift a restriction or send a substantive response on the controller's behalf without authority. If an instruction appears to breach data

protection law, immediately inform the controller and obtain appropriate advice; do not silently ignore it.

Where Social Value 360 is controller, the privacy lead assesses the request under Article 18. Restriction applies where accuracy is disputed while it is checked; processing is unlawful and the individual requests restriction instead of deletion; we no longer need the data but the individual needs it for legal claims; or an objection is being considered while the relevant grounds are verified. Record the applicable condition and decision. Respond without undue delay, normally within one calendar month. Use a lawful extension only where justified and notify the individual within the initial month, explaining reasons. Any refusal requires a documented lawful basis and an explanation of complaint and judicial remedy rights.

Identify exactly which records and activities are affected, the start time, permitted storage or other uses, review date, and who can authorise release. A restriction may affect only part of a record or particular uses; avoid stopping unrelated processing unnecessarily. Consider safeguarding implications with the DSL and relevant controller without assuming a blanket safeguarding exception.

Step 3 Apply the restriction across all locations

The privacy lead assigns the system and record owners to locate affected records in live systems, email, shared folders, paper files, exports, scheduled reports, supplier systems and backups. Use record identifiers and the data inventory; record each location checked. Stop affected automated workflows, communications, disclosures, analysis and routine use. Suspend scheduled deletion where needed to preserve restricted records.

Mark the records clearly as restricted with the incident or request reference, scope and authorising contact. Use technical controls such as blocked workflows, restricted permissions or a segregated secure location; a label alone is insufficient if ordinary use can continue. Secure and mark paper records and remove them from routine circulation. Keep a minimal suppression marker where needed to prevent re-import or accidental reuse.

Keep backup copies protected and outside ordinary use. Record how restrictions will be reapplied before restored data is made available. If a system cannot enforce the restriction, isolate or suspend the affected processing, escalate immediately to the privacy lead and the controller where relevant, and document the approved alternative. Do not claim completion while affected copies remain in routine use.

Step 4 Notify recipients and verify completion

Instruct relevant processors and sub-processors through an authorised secure route, require confirmation of the restriction and track outstanding responses. For Social Value 360 controller data, notify recipients to whom the affected data was disclosed unless this is impossible or involves disproportionate effort; document any such conclusion. Tell the individual about those recipients if requested. For data processed on behalf of another controller, coordinate recipient notifications with the controller and follow its instructions and contractual requirements.

The record owner tests that normal users and scheduled processes cannot use or disclose the affected information outside the permitted scope. Record the test, result, date and reviewer. Confirm to the controller what has been restricted, when, in which systems, any outstanding supplier actions and the next review. For our own controller data, communicate the decision and scope to the individual in clear, accessible language. Send no unnecessary personal data in confirmations.

Step 5 Maintain and review the restriction

Store restricted information securely and limit access to authorised people administering the restriction. Under Article 18, use beyond storage is permitted only with the individual's consent, for legal claims, to protect the rights of another natural or legal person, or for reasons of important public interest, as applicable. The privacy lead documents the lawful justification for any proposed

exceptional use; the controller's documented authority is also required where we act as its processor, subject to any applicable legal duty.

Set a case-specific review date and check outstanding restrictions at least monthly. A review date is not automatic permission to resume processing. Record access, exceptions, new copies, supplier confirmations and changes in circumstances. Treat unauthorised use of restricted data as a potential personal data breach and follow the Data Breach Policy.

Step 6 Lift only with authority and retain an audit trail

For data processed on behalf of another controller, lift the restriction only on the controller's verified documented instruction or an applicable legal requirement, informing the controller as required. For Social Value 360 controller data, the privacy lead records why restriction no longer applies and informs the individual before lifting it. Coordinate supplier and recipient updates and record when controls are changed. Reapply the retention schedule and any separate legal hold; do not automatically delete or resume every previous use.

Keep a restriction register containing the request reference, receipt and verification, controller and scope, decision and reasons, deadlines, locations and controls, owner, tests, recipient notifications, confirmations, permitted exceptions, review dates, release authority, advance notification and completion date. Retain decision records under the Data Retention Policy's rights-request category, with limited access and no unnecessary duplicate data.

The Privacy Lead arranges absence cover, maintains secure controller instruction routes, briefs personnel and tests restriction and release using a sample record without exposing personal information.

References

ICO restriction guidance: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-restrict-processing/>

ICO storage limitation guidance: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/>

Right-to-work retention: <https://www.gov.uk/check-job-applicant-right-to-work>

DBS handling guidance: <https://www.gov.uk/guidance/dbs-check-requests-guidance-for-employers>