



SOCIAL VALUE 360 LTD

Data Breach 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 must respond promptly to any loss, misuse or compromise of personal information. This policy applies to all staff, volunteers, contractors and approved processors and to paper, electronic, spoken, photographic and recorded information relating to participants, families, personnel and other people.

Report every actual or suspected breach immediately, even where the risk seems low or the information has been recovered. The incident coordinator arranges assessment of external notification; staff must not wait until they can prove harm.

Contacts and responsibilities

Initial reporting contact: Roy Ramrutton | roy@socialvalue360.co.uk | 07789 993621. IT response contact: Roy Ramrutton | 07789 993621. Safeguarding lead: Roy Ramrutton | 07789 993621.

Roy Ramrutton is the Privacy Lead, IT Lead and incident coordinator. He records incidents, assesses risk, coordinates containment and recovery, and makes or coordinates required notifications. The Responsible Director ensures cover, resources and timely decisions. Specialist IT support is engaged where needed. The safeguarding lead manages any risk of abuse, violence, exploitation or harm arising from a breach. Where roles are combined, significant decisions and technical recovery should receive a suitably competent independent check where practicable.

Where an email account or system may be compromised, use the verified telephone or another agreed secure channel. Do not send the incident details through the affected account. Urgent protection and statutory reporting must not wait for an unavailable manager or external adviser.

What counts as a breach

A personal data breach is a security failure resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal information. It includes an email sent to the wrong person, a missing paper file or device, inappropriate internal access, ransomware, an exposed shared folder or the loss of access to essential records.

Special category information includes health, ethnicity, religious beliefs and other Article 9 categories; biometric data is special category when used for unique identification. Criminal offence information has separate legal protections. Pseudonymised records remain personal information where people can be identified using additional information.

Immediate action by the person discovering the incident

1. Protect people first. Call 999 for immediate danger and alert the safeguarding lead if the incident creates a safeguarding risk.

2. Contact Roy Ramrutton on 07789 993621 immediately by a secure route. State what happened, when it was discovered, what information or systems are involved and what action has already been taken. Do not wait to complete a form.
3. Take safe, proportionate containment steps within your competence, such as stopping a disclosure, revoking an exposed link or disconnecting a suspected infected device from the network. Seek IT advice promptly. Do not wipe devices, delete logs or destroy evidence.
4. Preserve relevant times, messages and facts securely. Do not circulate the exposed information as proof. Follow instructions for recovery, password resets or contacting a mistaken recipient.
5. Do not independently make public statements, negotiate with attackers or promise an outcome. This does not prevent direct emergency referrals, protected disclosures or legally required reports.

Step 1 Identify and log the incident

Everyone must act on suspected loss, disclosure, alteration or unavailability of personal data. Warning signs include unexpected sign-in alerts, unexplained changes to records, missing attendance sheets, misdirected correspondence, unusual file downloads and reports from participants or suppliers. The IT lead reviews configured security alerts and backup failures; staff check recipients and sharing permissions and report mistakes or suspicious activity immediately. A report is required even if no harm has yet been established.

The first recipient of a report records the discovery date and time, reporter and safe callback details, affected service, brief facts and immediate action. The coordinator assigns a unique incident reference, records the separate time when there was a reasonable degree of certainty that personal data had been compromised, and starts the notification deadline log. If that time is uncertain, record the earliest plausible time and act conservatively. Record near misses too; if no personal data breach occurred, document the evidence and reasons.

Use the incident record at the end of this policy. Keep it in restricted organisational storage with an approved secure alternative available during an outage. Do not use a compromised account or enter incident details into unapproved AI tools. Reporting and containment run in parallel; completing the log must not delay protection or notification.

Step 2 Report and escalate immediately

If Roy cannot be reached, take safe containment steps within your competence, continue trying his telephone and email, and record each attempt. For data processed on behalf of another controller, notify that controller through the agreed incident route without waiting for internal approval. Obtain specialist technical assistance where needed. Roy, as Responsible Director, must arrange competent temporary incident responsibility during planned absences and ensure reporting deadlines are met. Call 999 for immediate danger; safeguarding referrals proceed alongside the data response.

Before personal data is processed on behalf of another organisation, the programme lead completes and makes available the following contact record: the controller's contract manager [Name, telephone and email]; the controller's information security or information governance incident route [Verified contact or reporting portal]. Keep the approved contact record accessible if normal systems fail. Verify these details against the agreement and the controller's instructions; do not guess an email address. If the dedicated route is unavailable, immediately alert the known contract manager, request urgent escalation and record attempts until receipt is confirmed.

For any actual or suspected information breach involving data processed on behalf of another controller, notify the controller immediately on discovery. Do not wait for an investigation, a completed form, a risk score or the 72-hour ICO deadline. Use the agreed secure route and follow up by telephone where urgent. Send the incident reference, discovery time, known facts, data and people potentially affected, immediate risks, containment taken and a safe contact. State what remains unknown. Share only necessary details; do not attach the exposed dataset routinely.

The coordinator obtains acknowledgement, records the controller's reference and agrees the next update time. Provide material new information promptly, with scheduled progress updates at least daily while the incident is active unless the controller requires a different frequency. Assist the controller with investigation, evidence, risk assessment, communications and reporting. Where another organisation is controller, that organisation decides its ICO and individual notifications; Social Value 360 supplies information promptly and acts on documented instructions. Separately assess any data for which Social Value 360 is itself controller.

Step 3 Contain and preserve evidence

The coordinator assigns an owner and deadline to each containment action. With authorised IT support, revoke exposed links and sessions, disable compromised accounts, isolate affected devices and correct permissions. For paper records, secure the area, trace the last location and arrange safe recovery. For a mistaken recipient, request no further use or sharing, secure return or deletion, and written confirmation; do not treat confirmation alone as proof that all risk has ended.

Preserve relevant logs, messages, access history and original records with dates, sources and a record of who handled the evidence. Authorised remote wiping or other destructive containment requires a documented assessment of immediate harm, evidence needs and available alternatives. Staff must not carry it out on their own initiative. Use competent technical assistance where the incident exceeds staff expertise.

Step 4 Assess and manage the risk

The coordinator opens an incident record immediately and records the time Social Value 360 became aware that a personal data breach had occurred. Investigation must be prompt; uncertainty must not be used to postpone the notification decision.

Assess the nature and sensitivity of the information, number of people and records, ease of identification, recipients, whether the data was accessed, effective encryption, recovery, duration and likely harm. Consider children, adults at risk, domestic abuse, financial fraud, discrimination, distress and loss of confidentiality. A small number of records can still create serious risk.

Contain the incident, establish the scope, preserve evidence, recover securely and record actions and owners. Consider related suppliers, accounts and ongoing access. Where Social Value 360 is a processor, notify the controller without undue delay and follow the processing agreement; do not apply our own ICO threshold before telling the controller. Processors acting for us must notify us without undue delay and assist the response.

Step 5 Decide and make external notifications

Where Social Value 360 is the controller, notify the ICO unless the breach is unlikely to result in a risk to people's rights and freedoms. Notification must be without undue delay and, where feasible, within 72 hours of awareness. This means elapsed hours, including weekends and holidays. Record the reasons for any delay.

Do not wait for all facts. An initial notification can be followed by information in phases without undue further delay. Provide the breach type, approximate affected people and records where possible, contact details, likely consequences and mitigation.

If the breach is likely to result in a high risk, tell affected people without undue delay in clear, accessible language. Explain what happened, likely effects, protective steps, our response and a contact for help. Do not wait for ICO permission where notification is required. Use safe contact methods, especially for children and people experiencing abuse.

Any exception to individual notification, such as effective encryption or measures that remove the high risk, must be assessed and recorded against the legal conditions. If direct communication would require disproportionate effort, use an equally effective public communication or similar measure as permitted by law.

Step 6 Recover and verify safe operation

Check contractual reporting times for commissioners and partners and notify insurers, relevant regulators or police where appropriate. Contractual notification does not replace ICO or individual notification. Share only necessary information and coordinate communications to avoid further disclosure.

Restore from verified clean systems and test security before reopening access. Keep an alternative way to deliver essential services and access emergency contacts. The Director authorises return to normal operation on advice from the response team and subject to the controller's instructions for data processed on behalf of another controller. The IT lead verifies that the cause is contained, access is appropriate, compromised credentials have been secured and restored records are accurate and usable. The service lead checks that essential participant and safeguarding services can operate safely. Record test results, authorisation and any continuing monitoring. Do not reconnect a system merely because it appears to work.

Step 7 Close the incident and prevent recurrence

Record all breaches, including those not notified externally: facts, consequences, assessment, decision and reasons, notifications, containment, recovery and actions. Keep this register restricted and follow the Data Retention Policy. Do not copy full exposed datasets into the register.

Within ten working days of stabilising the incident, the coordinator will arrange a review of the cause, effectiveness of response and required improvements. Assign actions and dates, test changes and report material risks to the Director. Review training, supplier terms and impact assessments where needed.

Before closure, the coordinator checks that containment and recovery are verified, notification decisions and communications are recorded, affected people have received required support, and remaining corrective actions have named owners and dates. Obtain the controller's confirmation of any required actions or handover for data processed on behalf of another controller. The Responsible Director records closure approval, date and residual risks; keep improvement actions open until checked. Reopen the incident if new evidence changes its scope or risk.

Personnel receive induction and annual refresher training. The Director tests incident reporting and response arrangements at least annually, including how urgent incidents are handled during absence. Deliberate or reckless breaches may lead to proportionate action under the applicable employment or contract process; good-faith reporting is encouraged.

Incident record template

Complete one restricted record per incident and update it throughout the response. Do not delay reporting to complete these fields.

Reference and status: [Reference; open, contained, recovering or closed].

Reporter and response owners: [Name, safe callback, coordinator, IT lead, safeguarding lead and approving Director].

Timeline: [Occurrence if known; discovery; organisational awareness; reasons for awareness time; notification deadlines and next review].

Facts and scope: [What happened; confidentiality, integrity or availability affected; systems; locations; recipients; data categories; estimated people and records; controller or processor role; facts still unknown].

Protection and containment: [Immediate risks to people; action; owner; time; result; further action needed].

Evidence: [Secure location; source; preservation action; access or handling history].

Risk and decisions: [Likelihood and severity of harm; vulnerabilities; encryption and actual access; reasons for ICO or individual notification or non-notification; decision owner; time; reassessment].

Notifications: [Relevant controllers; discovery report; acknowledgement and reference; ICO; affected people; police or other bodies; information supplied; delays and reasons; next update].

Recovery: [Cause; corrective steps; validation results; safe restart approval; continuing monitoring].

Closure and learning: [Support provided; remaining actions with owners and dates; the controller's requirements completed; closure approval and date; review meeting; retention review date].

Related policies and guidance

Read with Cyber Security, Data Retention, Safeguarding and both Privacy Notices. ICO breach guidance and reporting: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>