



SOCIAL VALUE 360 LTD

Cyber Security Statement and Policy

2026 to 2027 | Version 1.3

Policy owner: Roy Ramrutton, Responsible Director and IT 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 protects the confidentiality, accuracy and availability of information used to run its programmes and organisation. This policy applies to staff, volunteers, contractors and anyone using approved organisational accounts, devices, networks or services, including remote and community-based delivery.

The controls below are required operating standards. The IT lead keeps an inventory of actual systems and checks that each standard is implemented or has a documented, time-limited exception approved by the Director. Supplier names, storage locations and security certifications must not be assumed.

Responsibility and incident reporting

The Responsible Director owns cyber risk, approves resources and reviews significant issues. The IT lead or contracted provider manages technical controls and recovery. The privacy lead advises on personal data and the safeguarding lead on online harm, filtering and monitoring. Outsourcing IT does not remove Social Value 360's responsibility.

Main contact: Roy Ramrutton | roy@socialvalue360.co.uk | 07789 993621. IT emergency contact: Roy Ramrutton, IT Lead | 07789 993621. Roy Ramrutton is the Privacy Lead and IT Lead. These are operational roles and do not constitute appointment as a statutory Data Protection Officer. The organisation reviews whether a formal DPO appointment is required and, if so, ensures independence and absence of conflicting duties.

Report suspicious messages, lost devices, accidental disclosures, unusual sign-ins and system failures immediately. If a system may be compromised, use a verified telephone or safe alternative. Follow the Data Breach Policy where personal information may be affected and the Safeguarding Policy where someone may be at risk.

Accounts and access

Use individual authorised accounts and access only what your role needs. Do not share passwords or approve unexpected authentication prompts. Enable multi-factor authentication for email, cloud storage, finance, administrative and remote access wherever supported; the Director must approve compensating controls and a replacement plan where it is unavailable.

Use long, unique passwords or approved passkeys and an approved password manager. Change default credentials before use. Reset passwords when compromise is suspected or required for a justified security reason; routine calendar-based changes are not required.

Keep administrative accounts separate from daily work accounts. Review permissions at least quarterly and after role changes. Remove access promptly when someone leaves or no longer

needs it, recover equipment and transfer necessary records to an authorised owner. Do not preserve a leaver's entire mailbox indefinitely.

Devices and networks

Keep an inventory of devices, accounts, software and data owners. Use supported operating systems, automatic updates, device encryption, a firewall and appropriate anti-malware protection. Apply critical security fixes promptly under a documented risk-based schedule; isolate or replace unsupported systems.

Lock screens when unattended and configure automatic locking after a short period appropriate to risk. Protect devices during travel and avoid leaving them in vehicles. If unavoidable briefly, keep them concealed and locked; never leave sensitive devices or files in a vehicle overnight.

Use secure network settings and separate guest access from administrative systems. Remote access must use approved secure services and, where required by the design, a VPN. Do not expose remote administration directly to the internet without approved protection.

Personal devices require explicit approval, agreed separation of work data, security settings and a process to remove organisational access and information. Do not use shared family accounts or devices for confidential work.

Handling information and communications

Keep personal and confidential information in approved organisational storage. Use restricted links, verify recipients and check attachments before sending. Do not forward work records to personal email or use personal messaging, consumer cloud drives or unapproved removable media for sensitive work.

Use encryption in transit and on portable devices. If encrypted removable media are exceptionally authorised, record the purpose, owner and deletion date. Avoid unnecessary local downloads and printed copies. Keep paper records locked and dispose of them confidentially.

Check requests to change bank details or release sensitive records using a known, independently verified contact route. Do not rely on the telephone number in a suspicious message. Use separate approval for payments where practicable.

Cloud suppliers and new services

Before buying or using a service, identify its purpose, data, access model, hosting and support locations, subprocessors, security, backups, breach reporting, deletion and exit arrangements. The privacy lead checks controller and processor responsibilities, contractual protections and international transfers. Complete a data protection impact assessment where the processing is likely to pose high risk.

Do not place identifiable participant, safeguarding, personnel or commercially confidential information into unapproved AI tools. Approved uses require suitable terms, access controls, retention settings and human checking of outputs. AI must not make unreviewed safeguarding decisions or replace professional judgement.

Backups and continuity

Identify essential records and agree recovery priorities, acceptable data loss and restoration times. Back up important changing data at least daily unless a documented risk assessment justifies another frequency. Keep at least one protected copy separate from normal access, such as an offline or immutable backup, and restrict backup administration.

Check backup success and test restoration at least quarterly, recording results and corrective action. Synchronisation alone is not a backup. Protect and delete backup data in line with the retention schedule; information restored after deletion must be re-deleted where appropriate.

Maintain a continuity plan covering loss of email, internet, booking systems and key devices, with secure access to essential emergency contacts. Keep response contacts available outside the system they support. Exercise the plan annually.

Safe online delivery

Assess online activities for age, communication needs, participant vulnerability and the risks of harmful content, contact, conduct and commerce. Use approved platforms, controlled invitations, appropriate supervision and a clear route to report concerns. Staff use organisational channels and must not create private social media relationships with children they support.

The safeguarding lead and IT lead agree filtering and monitoring appropriate to the devices, venues and activities we control. Record who reviews alerts and how urgent concerns are escalated; do not assume a venue or supplier is monitoring on our behalf. Review effectiveness at least annually and after incidents. Explain any monitoring to users and assess privacy impacts.

Recording is off by default. An approved recording requires a defined purpose, lawful basis, advance information, restricted access and deletion date. Personal devices must not be used to photograph or record participants for work. Participants and families receive clear activity-specific guidance on safe online participation.

Responding to an incident

Stop unsafe activity and report immediately. Disconnect a suspected infected device from the network where safe, preserve evidence and obtain IT instructions. Do not erase files, negotiate with attackers or attempt unapproved recovery. Assess personal data and safeguarding risks promptly and apply the relevant reporting process.

The Director coordinates technical recovery, necessary notifications, participant communications and continuity. Reopen systems only after checks establish that recovery is safe. Record lessons, actions and owners.

Training and assurance

Provide cyber awareness training at induction and at least annually, including phishing, account security, safe sharing, incident reporting and online safeguarding. Use practical checks and supportive reporting so mistakes are raised early.

Quarterly management review covers access, updates, backup tests, supplier changes, incidents and outstanding exceptions. Review this policy annually and after significant changes. Staff acknowledge that they have read and understood it; any breach is considered fairly under the relevant conduct or contract process.

Reference guidance

National Cyber Security Centre small organisations guidance:

<https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security>

Password guidance: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach>