Date written: August 2025
Author: Catherine Scott
Date accepted by Board: September 2025
Publishing Quarter: October-December, 2025
Next Review Date: October, 2026

SCN Data Protection Policy

1. Purpose and Scope

The Social Change Nest CIC (SCN) is committed to protecting personal data and embedding privacy and accountability in all areas of our work. This policy outlines SCN's organisational approach to data protection in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all personal data processed by SCN, whether in digital or physical form. It applies to all SCN staff, contractors, volunteers, board members, and anyone acting on SCN's behalf.

This policy supports:

- Our Employee Privacy Notice
- Our External Privacy Notice
- Our IT Security Policy
- Our provision of services and operations.

SCN may also act as a data processor on behalf of funders or hosted collectives where applicable, and in such cases, we meet all contractual and legal requirements.

2. Roles and Responsibilities

SCN as Data Controller

SCN determines the purposes and legal basis for processing personal data. We are responsible for ensuring data is handled in accordance with data protection law.

Data Protection Lead (DPL)

The DPL provides oversight and guidance, monitors compliance, and serves as a point of contact for data subjects and regulators.

- General enquiries: hello@thesocialchangenest.org

- To report a concern or breach: reporting@thesocialchangenest.org

All individuals working with or on behalf of SCN must:

- Understand and follow this policy and supporting procedures
- Handle personal data lawfully, securely and with care
- Report breaches or concerns immediately

3. Data Protection Principles

SCN adheres to the key principles under UK GDPR. All personal data must be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Retained only as long as necessary
- Processed securely, maintaining confidentiality and integrity
- Handled in ways that uphold individuals' rights
- Evidenced and documented to demonstrate accountability
- Additional care is taken when processing children's data, and only with appropriate legal basis and guardian consent.

4. Lawful Basis for Processing

We process personal data only when there is a lawful basis (under Article 6 of UK GDPR) to do so. These may include:

- Consent – for newsletters or optional communications
- Contract – to manage grants, collective services, or other agreements
- Legal obligation – for regulatory, safeguarding or financial compliance
- Legitimate interest – in due diligence for funding/hosting, for communicating our work or improving our services
- Vital interest / public task – in rare and exceptional circumstances, such as protecting someone from serious harm or fulfilling a safeguarding duty, we may process data without consent. This is only done when necessary and proportionate, and where seeking consent would be unsafe or cause harmful delay.

5. Data Subject Rights

We uphold the following right for all data subjects:

- To access their personal data
- To request correction or deletion
- To restrict or object to processing
- To withdraw consent (where applicable)
- To raise a complaint with the Information Commissioner's Office (www.ico.org.uk)

Requests can be sent to: hello@thesocialchangenest.org
To report a concern confidentially: reporting@thesocialchangenest.org

6. Privacy by Design and Data Protection Impact Assessments (DPIAs)

We integrate privacy considerations into new systems, partnerships, or initiatives.

All individuals working with or on behalf of SCN must consult the DPL before:

- Launching tools that collect or process personal data
- Collecting special category data (e.g. health, safeguarding)
- Initiating large-scale or sensitive data processing
- Using automated decision-making or profiling
- Changing how, what, why or where publicly available personal data (e.g. screenshots from social media or web searches) is stored
- Any other changes or additions to use or processing of personal data

The DPL will assess if a Data Protection Impact Assessment (DPIA) is required and advise on completing it.

7. Data Retention

We retain data only as long as necessary for legal, contractual, or operational reasons. Typical retention periods include:

- Finance and grant records: at least 7 years (audit/legal requirements)
- General enquiries/forms: 2 years
- Contact data of clients: 7 years from the end of the financial year the relationship ended.
- Contact Data of Marketing & Newsletter Subscribers: Should there be no activity for a period of two years, an email will be sent to ascertain continued interest in receiving these communications. Should no opt-in be received within three weeks, the data will be deleted.
- Legal or safeguarding data: as required by law
- Due diligence data: at least 7 years

We securely delete or anonymise personal data once it is no longer needed.

8. Third-Party Processors

SCN uses trusted third-party tools and service providers (e.g. Google Workspace, HubSpot, BrightHR, Stripe, Wise) to support operations. We ensure that third parties:

- Meet UK GDPR and relevant security standards
- Enter into Data Processing Agreements where required
- Are reviewed regularly for risk, access, and necessity

Where data is transferred outside the UK or European Economic Area (EEA), SCN ensures safeguards such as Standard Contractual Clauses (SCCs) are in place.

9. Training and Awareness

All individuals working with or on behalf of SCN must:

- Complete data protection training on induction
- Complete refresher training annually (or as needed)
- Know how to report breaches and raise concerns
- Stay informed on best practices and regulatory updates

Managers are responsible for ensuring their teams meet these obligations.

10. Breach Management

A personal data breach includes unauthorised access, loss, theft, disclosure, or destruction of personal data.

All individuals working with or on behalf of SCN must report data breaches or near misses within 24 hours to: reporting@thesocialchangenest.org.

The DPL will:

- Log and assess the breach
- Notify the ICO and affected individuals within 72 hours if required
- Oversee any investigation, mitigation and remediation actions

11. Oversight and Review

This policy is owned by the DPL and reviewed at least annually, or sooner if:

- Legal or regulatory obligations change
- Significant operational or technology shifts occur
- Audits, breaches or internal reviews identify a need for revision

This policy should be read in conjunction with:

- SCN Employee Privacy Notice
- SCN External Privacy Notice
- SCN Legitimate Interests Assessment (LIA)
- SCN IT Security Policy
- SCN Whistleblowing Policy

Annex A: Glossary of Terms

Personal data
Any information that relates to an identified or identifiable individual. This includes names, email addresses, identification numbers, online identifiers (like IP addresses), and opinions linked to a person.

Data subject
The individual whose personal data is being processed. This could be a staff member, grantee, funder, partner, volunteer, or member of the public.

Data controller
The organisation or individual that determines the purpose and means of processing personal data. SCN is a data controller for the majority of our operations.

Data processor
A third party that processes personal data on behalf of the data controller under a contract. This might include cloud software providers, payroll services, or survey platforms.

Processing
Any activity carried out with personal data, including collection, storage, use, access, sharing, alteration, or deletion.

Special category data
Sensitive data that requires extra protection under the law. This includes data about health, race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, sex life, or sexual orientation.

Lawful basis
The legal grounds required under UK GDPR to collect and use personal data. These include consent, contract, legal obligation, legitimate interest, vital interests, and public tasks.

Legitimate Interests Assessment (LIA)

A Legitimate Interests Assessment (LIA) is a risk-balancing tool used to justify the use of legitimate interest as the legal basis for processing personal data under UK GDPR. It is required when processing personal data without consent, particularly in cases that may impact individuals, such as reviewing publicly available online information during due diligence.

DPIA (Data Protection Impact Assessment)

A documented risk assessment required for certain high-risk data processing activities. It helps ensure risks are identified and mitigated in advance (e.g. when introducing new technology or handling sensitive data).

ICO (Information Commissioner's Office)

The UK regulator for data protection. The ICO enforces compliance and upholds information rights for individuals (www.ico.org.uk).

Standard Contractual Clauses (SCCs)

Legal safeguards used when transferring personal data outside the UK or European Economic Area (EEA) to ensure equivalent data protection standards are upheld.