The Shalom Network

Data Protection Policy

Version 3.0	Approved
Document Owner:	Clive Paragreen
Approval Date:	04/08/2022
Latest Review Date	31/07/2023

The Shalom Network

1 Document Control

Document History

Date	Version	Version Author	Update Summary
03/05/21	1.6 (Draft) for Review and comment	Clive Paragreen	Set format, include TOC, material content update
09/05/21	1.7 (Draft) for Review and comment	Clive Paragreen	Content rationalised and simplified
10/05/21	1.8 (Draft) for Review and comment	Clive Paragreen	Further simplification. Minor content revisions following comment
13/05/21	1.9 (Final Draft) for Approval	Clive Paragreen	Minor content revisions following comment
07/07/21	2.0 Signed off version	Clive Paragreen	Title page updated as approved.
16/07/22	2.1 Draft for approval	Clive Paragreen	Minor updates including trustee changes
05/08/22	Version 3.0 Approved by Trustees	Clive Paragreen	No further amendments

Distribution

All approvers	For reference
Miriam Goldby	Subject Matter Expert for information
Jane Butler	Subject Matter Expert for information
Cheralyn Thompson	Subject Matter Expert for information

Approvers

Jess Thompson	Trustee
Lorraine Fellows	Trustee
Vic Knight	Trustee
Clive Paragreen	Trustee and Designated Data Protection Officer
Steve Thompson	Trustee

Storage and Retention

Current version to be present I the live document zone.
Archiving policy to be determined, currently on local hard drives and personal cloud storage.

The Shalom Network

CONTENTS

2 Our Data Protection Policy

The Shalom Network is serving people within the community having additional and specialised needs. We have a value driven commitment and legal obligation to safeguard those that we work with, walk alongside and support, many of whom are vulnerable. Our policies, procedures, training, as well as adherence monitoring and measures have been created and are maintained to keep people, safe from all kinds of harm including identity theft and cybercrime.

That's what it's about, keeping people safe from harm. This includes protecting the right to live in safety, free from abuse, unsolicited, unwelcome contact and criminal activity. We emphasise a preventative culture, as well as being clear and definite on managing policy failure should any incidents occur.

Failure to effectively manage personal data is unacceptable in any organisation, but even more so for one committed to serving those who are vulnerable and having its roots in Christian values.

3 Protection of Data – The Shalom Network **Policy Statement**

The Shalom Network will adhere to the Principles of Data Protection, as detailed in the Data Protection Act (DPA) 1998, the General Data Protection Regulation (GDPR) 2018 and any subsequent updates. Specifically personal data will be:

Processed lawfully, fairly and in a transparent manner in relation to individuals.

Collected for specified, explicit and legitimate purposes and not processed any further in a way that is incompatible with those purposes. Notable exceptions exist relating to, scientific or historical research, statistical purposes or where the public interest is served.

No more than adequate, relevant, and limited to what is necessary in relation to the purposes for which it is collected and processed.

Accurate and, up to date; with every reasonable step taken to ensure that it remains relevant to the purposes for which it is processed. Where found to be incorrect, erased or rectified without delay.

Kept in a form which permits identification of data subjects, for no longer than is necessary and for the purposes for which the personal data was collected and is processed.

Possibly stored for longer periods for archiving, scientific, historical research, statistical purposes or where the public interest is served. This subject to implementation of the appropriate technical and organisational measures required by the DPA and GDPR to ensure the rights and freedoms of individuals are preserved.

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and/or organisational measures.

The Shalom Network will also

Ensure that personal data is not transferred to a country or territory outside United Kingdom, or to another organisation unless that country or territory or other organisation ensures an adequate level of protection for the rights and freedoms of Individuals in relation to the processing of personal information.

Obtain permission of the data subject before any personal data is transferred, evidencing that any transfer is lawful and consistent with the purposes for which the data was originally collected and processed.

Ensure that the rights of people about whom information is held, can be fully exercised under DPA, GDPR and any other relevant legislation.

Not hold, or process on behalf of a third party, any individual's personal information, or sell or otherwise provide personal information/data to other organisations for their marketing or other purposes.

4 Designated Data Protection Roles

4.1 Trustees

The Shalom Network trustees are responsible for ensuring that the charity follows data protection law, whether that is the General Data Protection Regulation (GDPR), the Data Protection Act (DPA), or other relevant legislation. The Charity Commission's guidance is clear, trustees are responsible for ensuring that there are proper systems and processes in place to ensure that any activity that collects, stores and processes data is compliant.

They must also ensure that on-going monitoring is undertaken to evidence that this data protection policy and its supporting procedures are being effectively implemented in practice. This is critically important. Day to day responsibility is delegated to the Data Protection Manager and/or officers.

4.2 Designated Data Protection Manager

The Shalom Network is aware that regardless of whether the UK GDPR demands the appointment of a Data Protection Manager or Officer, that it must ensure that it has sufficient staff and skills to discharge its obligations under the UK GDPR.

Best endeavours will be made to appoint a suitably qualified Data Protection Manager or Officer who will be a trustee of The Shalom Network responsible for:

- Implementing the policy and all applicable related procedures and work methods.
- Ensuring The Shalom Network Data Protection policy is fit for purpose.
- Responding to requests for information about the policy from outside agencies, partners and data subjects.
- For policy and procedure reviews, amendments, and advice of changes to the team.
- Notifying trustees of items that require their attention and any approvals.
- Communication with and/or reporting to the relevant Regulators and authorities.

Whoever is appointed must have sufficient authority and independence within the charity to monitor all data processing, as well as having experience in data protection legislation.

They will be the first point of contact for the reporting of any incidents or concerns relating to data management and protection.

5 Policy Body

5.1 Risk and Risk Assessments

The Shalom Network Trustees have a duty to ensure effective risk management relating to its activities and to protect beneficiaries, donors, and team members It is also necessary to consider potential risks related to collection, storing and processing data from, and sharing data with third parties.

This policy considers potential risk to operational capability and credibility, reputation and assets of the Charity posed by the consequences of failure to adequately protect personal data. Effective data protection policies are a product of risk assessments being adequately carried out and interpreted.

The Shalom Network Trustees must ensure that the risks that arising from the Charity's activities and operations are regularly reviewed. They are also responsible for the development and maintenance of an appropriate risk register as well as the safeguarding policy and procedures.

Through implementation and rigorous adherence to the policy and supporting procedures, The Shalom Network will effectively manage the risks associated with its activities.

Management of risk and risk assessments is fully covered in The Shalom Network Correct Working Methods manual.

5.2 Disclosure

The Shalom Network may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The individual data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows The Shalom Network to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State.
- Protecting vital interests of an Individual or other person
- The Individual has already made the information public.
- Conducting any legal proceedings, obtaining legal advice, or defending any legal rights.
- Monitoring for equal opportunities purposes – i.e., race, disability, or religion.
- Providing a confidential service where the Individual's consent cannot be obtained or where it is reasonable to proceed without consent: e.g., where we would wish to avoid forcing stressed or unwell Individuals to provide consent signatures.

The Shalom Network regards the lawful and correct treatment of personal information as crucial to successful working, and to maintaining the confidence of all those with whom we are involved.

Further items relating to sharing data with third parties is laid out in section 5.4 of this document.

5.3 Data Collection – Informed Consent

Informed consent is when:

- An Individual clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data.
- And then gives their consent. The Shalom Network will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form, by email or other media.

When collecting data, The Shalom Network will ensure that the Individual:

- Clearly understands why the information is needed.
- Understands what it will be used for and what the consequences are should the Individual decide not to give consent to processing.
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
- Has received sufficient information on why their data is needed and how it will be used.

5.4 Data Storage

Personal information, data and records collected by The Shalom Network from any individuals will be stored securely and will only be accessible to authorised members of the team. Access management will be strictly managed with individual strong passwords subject to 30 day expiry/renewal periods.

Information will be stored for only as long as it is needed and will be disposed of appropriately thereafter.

It is the responsibility of The Shalom Network to ensure all personal and company data is non-recoverable from any device which has been passed on/sold to a third party, or the owner is no longer governed by this policy, where that device has previously been used within the organisation or on its behalf to store or manage personal data.

5.5 Data Access and Accuracy

All Individuals have the right to access the information The Shalom Network holds about them.

The Shalom Network will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, The Shalom Network will ensure that:

- It has a Data Protection Officer/Manager (a trustee), with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they have a responsibility for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised.
- Anybody wanting to make enquiries about handling personal information knows what to do.
- It deals promptly and courteously with any enquiries about handling personal information.
- It describes clearly how it handles personal information.
- It will regularly review and audit the ways it holds manages and use personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.

All staff are aware that a breach of this policy and/or the rules and procedures related to it may lead to disciplinary action being taken against them.

5.6 Subject Access Requests (SARS)

This policy recognises that The Shalom Network must respond effectively to SARs and has processes in place reflecting that:

- Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- This is commonly referred to as a subject access request or ‘SAR’.
- Individuals can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- In most circumstances, no charge or fee will be made to answer the request.
- Response should be given without unnecessary delay and within one month of receipt of the request.
- The response time may be extended by a further two months if the request is complex or if there are multiple requests from the individual.
- A reasonable search for the requested information must be carried out.
- The information provided should be in an accessible, concise and intelligible format.

- The information should be disclosed securely.
- Refusal to provide the information can only be made if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

The Shalom Network also:

- Must adequately assess if an individual is able to understand their rights and act accordingly.
- Has an emphasis on the need to use clear and plain language when disclosing information, particularly to children and those who may have specialised or complex needs.
- Will, deliver the information securely in an appropriate and wherever possible in the requestor's preferred format.
- Understands and acts upon the need to carefully consider a request from a third party made on behalf of an individual.
- Gives clear and justifiable reasons should a request need to be refused.
- Has a rigorous process to verify the identity of a requestor when and where appropriate.
- Has a procedure to record requests made verbally.
- Stores data in manner that facilitates retrieval in response to a request.

5.7 Correct Working Practice

The Shalom Network maintains and provides detailed methods and procedures to ensure correct working practices for all those across the Charity to follow when working and volunteering.

Further details are laid out in Appendix C, however, the full methods and procedures are contained in a separate document that is reviewed and updated more often than this policy document.

5.8 Incident Management

In the event of a report or allegation of The Shalom network failing in its obligations with regards to data protection it must be:

- Reported to the designated The Shalom Network Data Protection Manager or another trustee immediately.
- Handled and recorded in a secure and responsible way.
- Managed in accordance with The Shalom Network incident management policy and procedures.
- Actioned with urgency, ensuring further harm or damage is stopped or minimised.
- Reported to all relevant agencies and regulators in full where required.
- Communicated in a considered way to charity stakeholders and the wider public.
- Transparently managed, upholding The Shalom Network's reputation for acting with integrity.
- Reviewed by inquiry to understand root cause how to prevent a recurrence.
- Reported to the police if the incident or concern involves criminal behaviour.

5.8.1 Incident Log

A log will be kept of all incidents including data protection issues, it is confidential with access allowed by the Designated Officers, managers and trustees. Directly relevant sections will be released to others on a need to know, basis.

5.8.2 Incident Inquiries and Reports

A comprehensive inquiry must be held following an incident or allegation. Any inquiry process should be handled objectively, sensitively, and sympathetically. Involvement should be restricted to essential persons only, but as a minimum a data Protection officer and/or a trustee should preside alongside involved parties and/or their representatives.

A concise report must be produced and reviewed by the data protection manager and a decision made as to whether the matter needs to be referred to the trustees or outside authorities (see below).

Any required action or improvement plan must be documented, sponsored by a trustee and its progress tracked to ensure satisfactory completion.

The Trustees acknowledge their duties to make a Serious Incident report to the appropriate authorities that there has been an incident (alleged or actual), which is in breach of data protection policy and potentially law within the context of the The Shalom Network's activities.

The Shalom Network has relevant procedures detailed in The Shalom Network Correct Working Methods.

5.9 Monitoring and Measuring Policy Effectiveness

Constant monitoring takes place with the need to be observant, aware and diligent. Points of note should be shared, and any required actions raised in colleague briefings, colleague performance management reviews and Feedback sessions.

Any incident, reportable or otherwise is investigated and analysed. If that investigation process reveals a deficiency, an improvement plan is created and progressed.

5.10 Related Policies and Other Artefacts

This policy references a number of other policies and procedures that have been created and are maintained with regard to safeguarding demands.

- The Shalom Network Correct Working Methods
- The Shalom Network Risk Register

5.11 Maintaining the Policy

This policy will be updated as necessary to reflect best practice in data management, security, and control as related to the activities of The Shalom Network. It will be maintained, reviewed and when amended as necessary to ensure compliance with any changes or amendments made to the Data Protection Act 1998, General Data Protection Regulation, and any other relevant legislation.

Whilst The Shalom Network trustees have a responsibility to review, with designated team members and agree this policy at least annually, the possible need for interim reviews and updates is acknowledged.

The Data Protection Manager will, be responsible for reviewing the policy in the light of material legislative and operational changes. They will work with other team members to review and recommend any actions to the trustees.

Where a review dictates material changes to the policy a working group should be formed to update the policy document to a draft revision for approval by the trustees and Designated Safeguarding Officers. The detail of any changes should, where required, be reflected in any guidance and training material. Team

The Shalom Network reserves the right to amend this Policy from time to time at its sole discretion. This policy recognises the diverse needs of individuals and The Shalom Network will use multiple communication and media channels to give notice of any change prior to it becoming effective.

If as the result of such changes, any individual would like to amend their instructions with regard to how The Shalom Network uses their Personal data, they can do so typically, but not exclusively by emailing information@theshalomnetwork.org.

A. Appendix A – Contact Details

Designated Data Protection Manager

Clive Paragreen (Data Protection Officer)	**Mob:** 07432201490 **Email:** cliveparagreen@theshalomnetwork.org.uk

Trustees

Clive Paragreen (Chair)	**Mob:** 07432201490 **Email:** cliveparagreen@theshalomnetwork.org.uk
Jessica Thompson (Vice Chair)	**Mob:** 07432201490 **Email:** jessthompson@theshalomnetwork.org.uk

B. Appendix B – Terms and Definitions

Third Party

The term **'third party'** relates to a person or group besides the two primarily involved in a situation. For example, party one = The Shalom Network, party two = The Shalom network beneficiaries, party three = suppliers and partner organisations.

Data Subject

GDPR defines '**data subjects**' as "identified or identifiable natural person[s]." In other words, **data subjects** are in fact people—human beings from whom or about whom information is collected in connection with an organisations business and its operations.

Team

Within the context of The Shalom Network's documentation, **'team'** is the collective term covering, employed, contracted and volunteer colleagues engaged in carrying out the charity's activities.

Beneficiary

A **beneficiary** is anyone who uses or benefits from a **charity's** services or facilities, whether provided by the **charity** on a voluntary basis or as a contractual service, perhaps on behalf of a body like a local authority.

C. Appendix D – Summary of Referenced Documents

The Shalom Network Correct Working Methods

- Responsibility and Accountability
- Risk Assessments and Risk Management
- Recording Attendance
- Transport
- Social Media
- Online
- Contact and Communication.
- Resourcing and Resource Planning
- Events
- Group Meetings
- Reporting
- Personal and Property Security
- Work Methods
- Collecting, Processing, Storing, Securing and Deleting Personal Information
- Sharing Data
- Data Retention
- Storage and Archiving
- Access Controls
- Incident Management
- Purchasing, payments and expenses
- Collecting, recording, and allocating donations
- Gift aid
- Grant applications
- Sponsorship
- Work records, training register and skills matrices.

The Shalom Network Risk Register

- Risk description and reference
- Date recorded.
- Owner
- Priority Level
- Status, e.g., ‘Open’, ‘Accepted’
- Outline action plan
- Planned remediation date.