SIKH SANJOG

POLICIES DOCUMENT

2026 Edition

Sikh Sanjog
3 Coalhill, The Shore, Leith
Edinburgh EH6 6RH
Email: admin@sikhsanjog.com
Website: www.sikhsanjog.com

Version 1: 2026 Edition
Date of Issue: March 2026
Review Date: Annually
Approved by: Managing Director, *Trishna Singh OBE*
Director of Operations: *Jess Kaur Panesar*

2. CONFIDENTIALITY POLICY

2.1 Policy Statement

Sikh Sanjog is committed to protecting the privacy, dignity, and personal information of all staff, volunteers, and service users. Confidentiality is central to building trust, safety, and meaningful relationships within our community.

Our approach reflects Sikh values of respect, integrity, and collective responsibility. We recognise that many individuals who engage with our services may share sensitive information, often in moments of vulnerability. It is our duty to handle this information with care, professionalism, and cultural sensitivity.

2.2 What Is Confidential Information?

Confidential information includes any personal or sensitive details shared with Sikh Sanjog in trust. This may include, but is not limited to:

- Personal details: Names, addresses, contact information, family details, or any information that can identify an individual
- Case notes: Information gathered during support, outreach, or wellbeing sessions
- Health information: Any physical or mental health details shared in confidence
- Group discussions: Information shared within women's groups, men's groups, youth sessions, or community circles, where participants expect privacy
- Counselling or support session notes: Written or verbal information shared during therapeutic or emotional support
- Financial or immigration information: Any details relating to benefits, employment, immigration status, or financial hardship
- Digital information: Emails, messages, or online communications shared with staff or volunteers

Confidential information must always be treated with respect and stored securely.

2.3 When Confidentiality May Be Broken

While Sikh Sanjog is committed to maintaining confidentiality, there are circumstances where information must be shared to protect individuals or comply with the law. Information may be shared without consent if:

- Someone is at risk of harm (including self-harm, harm to others, or risk from another person)
- A crime has occurred or is likely to occur

- There is a safeguarding concern involving a child or adult at risk
- The law requires disclosure (e.g., court orders, police investigations)

Information may also be shared with consent when the individual agrees that sharing will support their wellbeing or access to services.

If staff are unsure whether confidentiality should be broken, they must seek guidance from the Safeguarding Lead, senior management, or relevant authorities before taking action.

2.4 Staff Responsibilities

All staff and volunteers have a duty to protect confidential information. This includes:

Secure Storage

- All confidential information must be stored using Sikh Sanjog's secure systems.
- No confidential documents may be stored on personal devices, including laptops, phones, or USB drives.
- Paper records containing confidential information must not be left unattended at any time and when not in use must be kept in locked cabinets accessible only to authorised staff.

Use of Approved Systems

- Staff must use only work-approved platforms for emails, case notes, and communication.
- Personal email accounts, messaging apps, or social media must never be used for work-related confidential information.

Professional Conduct

- Case discussions must take place in private spaces where they cannot be overheard.
- Staff must be mindful of confidentiality when working in shared offices, community spaces, or public areas.
- Confidential information must never be shared or discussed with friends, family, or anyone outside the organisation.

Reporting Breaches

- Any suspected or actual breach of confidentiality must be reported to management immediately.

- Early reporting allows the organisation to contain the issue, support those affected, and take corrective action.

2.5 Upholding Sikh Sanjog's Values

Confidentiality is not only a legal requirement, but also a reflection of our commitment to:

- Respecting every individual's dignity
- Creating safe and trusting spaces
- Honouring cultural sensitivity and lived experience
- Supporting empowerment and autonomy

By protecting confidentiality, we ensure that Sikh Sanjog remains a place where people feel safe to share, heal, and grow.

3. DATA PROTECTION / GDPR POLICY

3.1 Introduction

Sikh Sanjog is committed to protecting the personal data of all staff, volunteers, service users, partners, and community members. We comply fully with the UK General Data Protection Regulation (GDPR) and all relevant UK data protection laws.

Our approach reflects Sikh values of integrity, respect, and collective responsibility. We recognise that many individuals share sensitive information with us during times of vulnerability, and we have a duty to handle this information with care, transparency, and professionalism.

This policy outlines how Sikh Sanjog collects, stores, uses, and protects personal data.

3.2 Data Protection Principles

Sikh Sanjog adheres to the seven core GDPR principles. All staff and volunteers must ensure that personal data is:

• **Lawful** - Collected and processed only when there is a clear legal basis.

• **Fair** - Handled in ways that respect the rights and dignity of individuals.

• **Transparent** - People must understand what data we collect, why we collect it, and how it will be used.

• **Limited to what is necessary (Data Minimisation)** - We only collect information that is essential for delivering our services safely and effectively.

• **Accurate** -Information must be kept up to date and corrected promptly when needed.

• **Secure** -Data must be stored safely, protected from loss, misuse, or unauthorised access.

• **Retained only for as long as necessary** - We keep data only for the period required by law or organisational need, after which it is securely destroyed.

These principles guide all our decisions and reflect our commitment to safeguarding the trust placed in us.

3.3 What Data We Collect

Sikh Sanjog collects only the information necessary to provide safe, effective, and culturally sensitive services. This may include:

Personal Information

- Name, address, phone number, email
- Date of birth
- Emergency contact details

Health and Wellbeing Information

- Physical or mental health information
- Support needs
- Relevant medical or accessibility information

Case Notes and Support Records

- Notes from wellbeing sessions, outreach, or community support
- Information shared during group work or one-to-one support

Volunteer and Employee Information

- Application forms
- Training records
- HR documentation
- Performance, conduct and supervision notes

Other Relevant Information

- Attendance records
- Consent forms
- Photographs or media (only with explicit consent)

We collect this information to ensure safety, provide appropriate support, and meet legal and funding requirements.

3.4 Responsibilities of Staff & Volunteers

All staff and volunteers have a legal and ethical responsibility to protect personal data. This includes:

Secure Use of Devices

- All devices must be password protected.
- Work laptops and phones must be locked when unattended.
- Personal devices must never be used to store or process confidential information.

Secure Storage

- Digital files must be stored on Sikh Sanjog's secure systems.
- When not in use, Paper records must be kept in locked cabinets accessible only to authorised staff
- When in use, paper records containing personal information must not be left unattended

Access Control

- Staff may only access information relevant to their role.
- Curiosity or informal access is strictly prohibited.

Reporting Breaches

- Any suspected or actual data breach must be reported immediately to management.
- Early reporting helps protect individuals and ensures compliance with GDPR.

Professional Conduct

- Personal data must never be discussed in public spaces or shared informally.
- Staff must always follow confidentiality and safeguarding procedures.

These responsibilities ensure that Sikh Sanjog remains a safe and trusted organisation.

3.5 Data Retention

Sikh Sanjog retains data only for as long as necessary and in line with legal requirements:

Type of Record	Retention Period
Service user records	7 years
HR and volunteer records	6 years
Financial records	6 years
Safeguarding records	In line with statutory guidance (minimum 7 years)

After the retention period, data is securely destroyed in accordance with GDPR standards.

3.6 Upholding Sikh Sanjog's Values

Our data protection practices reflect our commitment to:

- Dignity and respect for every individual
- Cultural sensitivity in how information is gathered and used
- Transparency and honesty in our communication
- Empowerment by ensuring individuals understand their rights
- Collective responsibility for safeguarding our community

By protecting personal data, we honour the trust placed in us and uphold the values that guide our work.

3.6 Data Breach Flowchart