DATA PROTECTION POLICY

SALMA ATTAH FOUNDATION FOR WOMEN AND GIRLS SUPPORT

Version 1.0 | November 2026

Copyright © 2026 Salma Attah Foundation for Women and Girls Support (SAFWGS), Nigeria. All rights reserved.



Data Protection Policy

Version 1.0 | Approved November 2026 | Next review November 2027

Purpose

SAFWGS collects personal information from the women, girls, parents, survivors, fellows, volunteers, staff, donors and partners it works with. Much of it is sensitive: information about health, menstrual health, experiences of violence, location, age and family circumstances. If it is lost or misused, people can be harmed.
This policy sets out how SAFWGS collects, uses, stores, shares and deletes personal data, in line with the Nigeria Data Protection Act 2023 (NDPA) and the regulations and directives of the Nigeria Data Protection Commission (NDPC).

Scope

This policy applies to the Board, staff, interns, fellows, volunteers, consultants and partners who handle personal data for SAFWGS, in any form: paper forms, spreadsheets, databases, email, WhatsApp, photographs, audio, video, online forms, digital tools and AI tools.

Key terms

Personal data: any information that identifies a person directly or indirectly, such as a name, phone number, photograph, voice, address, school, ID number or a combination of details.
Sensitive personal data: data about health (including menstrual and reproductive health), sex life, religious or other beliefs, ethnicity, political opinions, trade union membership, biometric and genetic data, and criminal records. SAFWGS also treats information about gender-based violence, safeguarding concerns and children as requiring the same high level of protection.
Data subject: the person the data is about.
Processing: anything done with personal data, including collecting, recording, storing, using, sharing, analysing and deleting it.
Data breach: any loss, theft, unauthorised access, disclosure, alteration or destruction of personal data.

Data protection principles

SAFWGS processes personal data only when it:

- Is lawful, fair and transparent: people are told what we collect and why, in a language they understand
- Is for a specific, legitimate purpose and not used for something unrelated
- Is limited to what is needed for that purpose
- Is accurate and kept up to date
- Is kept no longer than needed
- Is kept secure against loss, theft and unauthorised access
- Can be shown to meet these principles, through records and accountability

Lawful basis

SAFWGS relies on one of the lawful bases in the NDPA for each use of personal data, most often:

- **Consent:** for programme registration, photographs and stories, newsletters, research and digital tools
- **Contract:** for employment, volunteer, consultancy and supplier arrangements
- **Legal obligation:** for tax, pension, audit and reporting duties
- **Vital interests:** where someone's life or safety is at serious risk
- **Legitimate interests:** for limited activities such as keeping donor records, where this does not override the person's rights

Sensitive personal data is processed only with explicit consent, or where the law allows it to protect someone's vital interests or to establish or defend legal claims.

Consent

- Consent must be freely given, specific, informed and recorded. A signature, thumbprint, tick box or recorded verbal consent is acceptable where documented
- People must be told who SAFWGS is, what data we collect, why, who we share it with, how long we keep it, and how to withdraw consent or contact us
- For children under 18, consent comes from a parent or guardian, together with the child's own agreement, as set out in the Child Safeguarding Policy
- No one may be refused a service because they decline to have their photograph taken or their story used
- People can withdraw consent at any time by contacting info@safwgs.org or +234 813 693 1762

Rights of data subjects

Everyone whose data SAFWGS holds has the right to:

- Be informed about how their data is used
- Access a copy of their data
- Have inaccurate data corrected
- Have their data deleted where there is no longer a lawful reason to keep it
- Restrict or object to certain uses of their data
- Receive their data in a portable format where this applies
- Withdraw consent
- Complain to the Nigeria Data Protection Commission

Requests can be made in any form, including verbally, to any staff member or to info@safwgs.org with the subject line "Data Protection Request". SAFWGS will verify the person's identity and respond within 30 days.

How SAFWGS handles data in its programmes

Programme participants and fellows

- Registration forms collect only what is needed to deliver and report on the programme
- Reports to funders use anonymised or aggregated data unless the funder has a legitimate need for names and participants have agreed
- Attendance and payment lists are stored securely and are not shared in public WhatsApp groups

Survivors and safeguarding cases

- Information about violence, abuse or safeguarding concerns is recorded only by the designated safeguarding officer and stored separately, with access limited to those who need it
- Survivors' information is shared with service providers only with their consent, except where there is a serious risk to life or to a child

Digital tools, helplines and chat services

For any SAFWGS digital tool, including the planned SafeSisi+ service and any WhatsApp, SMS or chat-based support:

- A data protection impact assessment is completed before launch
- Users are told clearly, at the start, what is recorded, who can see it and how long it is kept
- The minimum data is collected, and anonymous use is allowed wherever possible
- Conversations are stored on accounts controlled by SAFWGS, with access limited to named staff
- Third-party providers sign a data processing agreement
- Disclosures of harm are handled under the safeguarding policies

Accountability and civic participation work

In accountability projects, such as community budget tracking and The Money Trail, SAFWGS may collect information from citizens and reports about public spending. SAFWGS will protect the identity of community members and sources, publish only information about public institutions and public funds, verify information before publishing it, and not publish personal data about individuals beyond what is needed to report on a public office.

Photographs, video and stories

Media is handled under the Communication and Visibility Policy and the consent rules above.

Staff, volunteers and job applicants

Personnel files, payroll data and recruitment records are held securely with limited access under the HR Policy. Unsuccessful applicants' data is deleted within 12 months unless they agree to it being kept.

Donors and supporters

Donor and supporter data is used only to process gifts, thank donors, meet legal obligations and, with consent, send updates. SAFWGS never sells or rents personal data.

Security

- Use SAFWGS accounts (safwgs.org email and approved shared drives), not personal email or personal cloud storage, for SAFWGS data
- Switch on two-step verification for all SAFWGS email, drive and social media accounts
- Protect laptops and phones with a password or PIN, keep software updated, and lock screens when away
- Share files by restricted link with named people, not "anyone with the link", when they contain personal data
- Keep paper forms in a locked cabinet, and transfer field forms to the office promptly
- Move photos and forms from personal phones to SAFWGS storage and delete them from the phone within 7 days
- Remove access for anyone who leaves SAFWGS on their last day
- Never enter personal or sensitive data about participants into public AI tools (see the AI Use Policy)

Sharing data

SAFWGS shares personal data only where there is a lawful basis and a clear need, and only the minimum required. Partners, consultants and service providers who process data for SAFWGS sign a data processing or data sharing agreement that requires them to protect it, use it only for SAFWGS's purpose, and return or delete it at the end. Data is transferred outside Nigeria (for example to a cloud service or a funder) only where the NDPA's conditions for cross-border transfers are met.

Retention

- **Programme registration and attendance records:** the length of the project plus the period required by the funder, normally 7 years
- **Safeguarding records about a child:** until the child turns 25, or 6 years after the case is closed, whichever is later
- **Other safeguarding and whistleblowing records:** 6 years after closure
- **Financial records:** 7 years
- **Personnel files:** 6 years after employment ends
- **Unsuccessful job applications:** 12 months
- **Consent forms for photos and stories:** as long as the material is in use, plus 6 years
- **Chat and helpline conversations:** no longer than needed to provide support and follow up, as set in the tool's impact assessment

At the end of the retention period, paper records are shredded and digital records are permanently deleted, or anonymised if needed for statistics.

Data breaches

Anyone who discovers or suspects a data breach, such as a lost phone with participant photos, an email sent to the wrong group, or a hacked account, must report it immediately to the Data Protection Officer at info@safwgs.org with the subject line "URGENT – Data Breach", and by phone on +234 813 693 1762.
The Data Protection Officer will contain the breach, assess the risk, and record it in the Breach Register. Where the breach is likely to risk people's rights and freedoms, SAFWGS will notify the Nigeria Data Protection Commission within 72 hours of becoming aware of it, and will tell the affected people without delay where the risk to them is high, explaining what happened and what they can do. Affected funders are informed as their agreements require.

Roles

- **Board:** approves this policy and receives an annual data protection report
- **Executive Director:** is accountable for compliance and appoints the Data Protection Officer
- **Data Protection Officer:** advises staff, keeps the record of processing activities, the Breach Register and data sharing agreements, handles data subject requests, leads training, and manages registration and filings with the NDPC where SAFWGS is required to make them
- **Project leads:** make sure their projects follow this policy and complete impact assessments for new tools
- **Everyone:** handles personal data carefully and reports breaches straight away

Data Protection Officer: contact through info@safwgs.org or +234 813 693 1762 (subject “Data Protection Request”)

Training

All staff and volunteers receive data protection training during induction and a refresher each year.

Related policies

- Child Safeguarding Policy
- Adult Safeguarding and PSEA Policy
- AI Use Policy
- Communication and Visibility Policy
- HR Policy
- Whistleblowing Policy

Approval

Approved by the Board of SAFWGS in November 2026. This policy will be reviewed in November 2027, or earlier if the law, NDPC guidance, a funder requirement or SAFWGS's work changes.

Approved by the Board of Trustees of SAFWGS by resolution dated 12 November 2026. Signed copies are held by SAFWGS and are available to funders and partners on request.