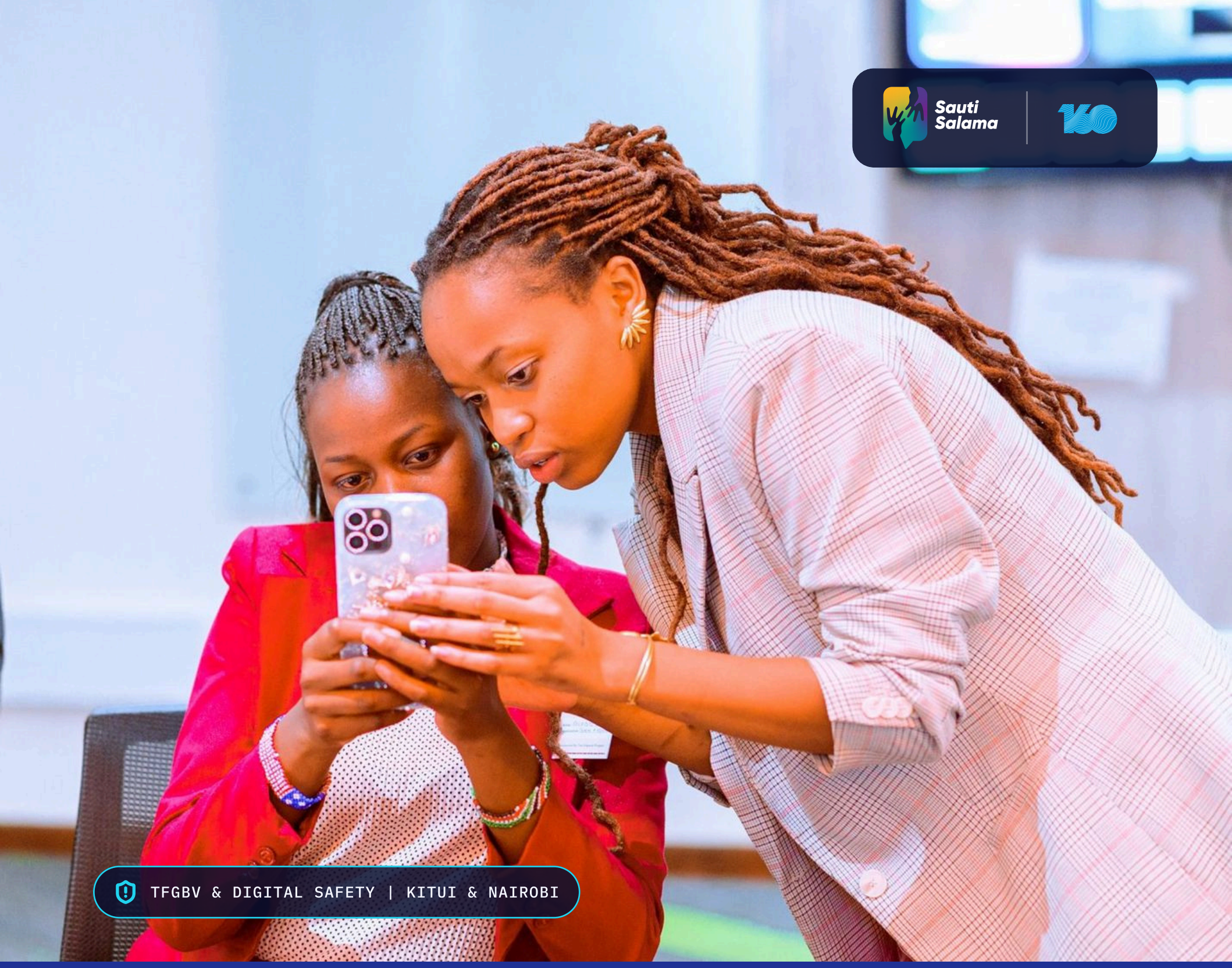


POLICY BRIEF | 2026

219 RESPONDENTS / 6 KIIs / 2 FGDs

Safe Digital Futures

Understanding young women's online safety and digital tool use in Kenya. A mixed-methods study under the ITU160 Gender Champions Initiative, August 2026.

PUBLISHED BY SAUTI SALAMA | PREPARED UNDER THE ITU160 GENDER CHAMPIONS INITIATIVE

Sauti Salama

PUBLISHED BY SAUTI SALAMA | PREPARED UNDER THE ITU160 GENDER CHAMPIONS INITIATIVE

PHOTOGRAPHY: ITU160 Gender Champions.

ABOUT & CONTENTS

A survivor-led voice for safety.

Sauti Salama operates at the nexus of technology, community response and legal advocacy: a trusted, inclusive space where people can report harm without fear, access dignified support, and move through clear pathways to help. This brief turns research on young women's digital safety into policy that government, platforms and civil society can act on.

In this brief

01 Executive summary & the numbers 03

02 Methodology, scope & the study sample 04

03 Glossary of key terms 05

04 Evidence I: harm is routine; prevention is the loudest ask 06

05 Evidence II: enforcement, capacity & platform transparency 07

06 Evidence III: the AI legal gap, repeat abuse & younger women 08

07 Policy options 09

08 Recommendations by actor 10

09 The platform in practice 11

10 Conclusion & references 12

Online harm against young women is not a marginal problem.

Three findings anchor this brief: online harm is routinely normalised and dismissed; awareness and education is the most demanded intervention; and respondents want enforcement of existing law more than new law.

42%

Have personally experienced online violence or abuse

91 of 219 respondents, consistent with a 2023 UNFPA study.

98%

Use the internet several times a day

50%

Who were harmed did not report it

They did not believe it would help, the largest barrier.

74%

Want stricter enforcement of existing law

The most requested change of all.

64%

Would report abuse to the platform

But only 16% would seek help from an organisation.

METHODOLOGY & SCOPE

A concurrent mixed-methods study, triangulated across sources.

The study combines a structured online survey of 219 respondents aged 16 to 35, six Key Informant Interviews, and two Focus Group Discussions held in Kitui and Nairobi, conducted July to August 2026.

Key informants spanned a case manager at CREAW, an independent GBV legal practitioner, an advocacy officer at FIDA Kenya, a research officer at the ODPC, a senior digital-skills trainer at Nairobits, and two legal researchers at CIPIT.

All qualitative material, including the survey's open-ended question, was coded against a shared codebook of nine thematic domains and 45 codes, so findings could be checked for consistency across methods.

Where sources agree, a finding is treated as well-triangulated; where they genuinely disagree, that disagreement is presented as a policy option.

The scope is technology-facilitated gender-based violence and digital safety among young women in Kenya specifically. It does not address online harm to men and boys, or cybercrime unrelated to gender, except where these intersect with the findings.

THE STUDY SAMPLE

219 women surveyed, aged 16–35

88% rate a digital-safety resource highly useful

6 Key Informant Interviews across law, advocacy, regulation & platforms

2 Focus Group Discussions, in Kitui & Nairobi

The language of technology-facilitated harm.

Technology-facilitated gender-based violence (TFGBV)

An act of violence committed, assisted, aggravated or amplified in part or fully through information and communication technologies or digital media, against a person on the basis of their gender.

Doxxing

Sharing a person's personal information, such as a home address or phone number, without consent, to enable harassment or intimidation.

Cyberstalking

Persistent, unwanted or threatening surveillance or contact carried out through digital means, which may extend into offline stalking.

Non-consensual intimate images

Sharing or publishing intimate images or videos of a person without consent, including where the images were originally created consensually.

Sextortion

Extorting a person by threatening to disseminate their intimate images or information unless a demand, financial or otherwise, is met.

Deepfake

Digitally manipulated image, audio or video content, often generated using artificial intelligence, that convincingly depicts a person saying or doing something they did not do.

Harm is routine and dismissed, and prevention is the loudest ask.

01

Online harm is routine, and frequently dismissed as unimportant

Harm normalisation is the most common pattern across the qualitative dataset. The core problem is recognition, not incidence: many did not know what they experienced was violence until it was named. Half of survivors did not report, believing it would make no difference.

“Most violent threats aren’t taken seriously and are dismissed as jokes. I’ve been threatened with rape and no one took it seriously.”

SURVEY RESPONDENT | OPEN-ENDED QUESTION

02

Awareness and education is the most consistently requested intervention

Calls for digital-safety education are the strongest single pattern in the entire dataset, appearing in every interview, both focus groups, and 52.1% of survey responses. Practitioners at very different points in the system converged on the same diagnosis.

“Prevention is key, and there’s a real gap there. We need a lot more awareness creation in the community around the safe use of gadgets.”

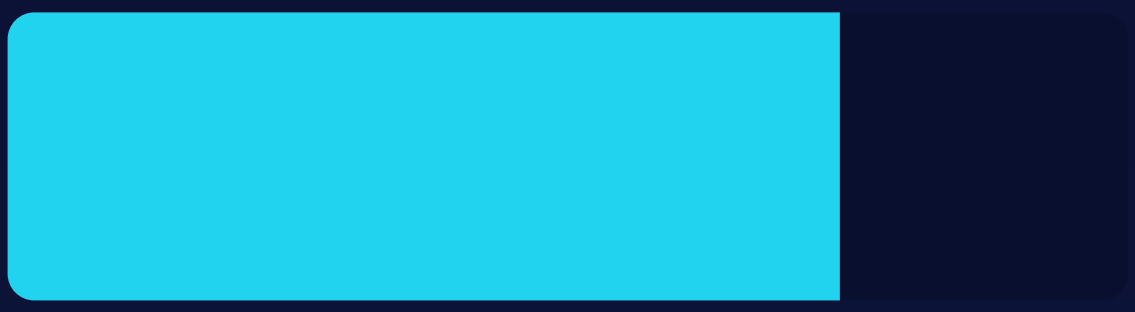
CASE MANAGER | CREAW



Respondents want enforcement of existing law, more than new law.

Share of 219 survey respondents selecting each change as something that would make them feel safer online.

74.4%
Stricter enforcement of harassment laws



58.4%
Greater platform transparency on data



55.3%
Easier in-app reporting



52.1%
More digital-safety education



03

Institutional capacity is a distinct gap

Across five independent sources, police and courts are not equipped, in training or attitude, to receive technology-facilitated cases.

“They might say, ’I’m dealing with murder cases here.’”

FIDA KENYA

04

Platform transparency is population-level

Raised in both focus groups and, independently, by 58.4% of the full survey sample, a broad demand rather than an artefact of small groups.

“Regulations already exist on paper. What’s missing is implementation.”

FGD2 | NAIROBI

A nameable legal gap, repeat abuse, and withdrawal from public life.

05

A specific, nameable legal gap around AI-generated content

Legal experts agreed Kenyan law does not adequately address deepfakes. Where a tool is used to create fake images, more than one party is responsible, but the law as drafted reaches only the primary violator. Anonymous and pseudo-accounts also enable repeat abuse, named as a specific platform design failure: blocking should link an abuser's other accounts.

06

Impact compounds, and includes withdrawal from public voice

Impact spans psychological, economic, social and educational domains and compounds over time. A distinct consequence is self-silencing: repackaging advocacy, or disappearing entirely. Only 14.6% would leave a platform immediately, against 83.1% who block and remain, so withdrawal reads as a slow, cumulative response to sustained harm.

07

Younger women are named as most vulnerable; data must catch up

Every qualitative source describes younger women and girls facing grooming risk and inexperience online. The survey cannot yet confirm this: the 16–18 bracket rests on only 3 of 219 respondents, a sampling gap flagged here rather than smoothed over.

POLICY OPTIONS

What the law covers, where it falls short, and three ways forward.

AREA	CURRENTLY ADDRESSED	GAP IDENTIFIED IN THIS STUDY
Data misuse & privacy	Data Protection Act 2019; ODPC complaints process with a 90-day window.	Complaints not sex-disaggregated; GBV cases fall outside the mandate.
Harassment & doxxing	Computer Misuse & Cybercrimes Act 2018 covers cyber harassment.	"Obscene" and "intimate" undefined, weakening prosecution.
AI & deepfake content	General provisions may reach the primary violator.	No liability for those who build or supply the enabling tools.
Enforcement capacity	Police gender desks exist for GBV reporting.	Training does not extend to technology-facilitated cases.



OPTION A

Prioritise new or amended legislation

Addresses the root with one unambiguous legal category, but reform is a multi-year process that leaves the current gap open meanwhile.

OPTION B

Prioritise enforcement & public legal awareness

Actionable now and matches the top-requested change, but cannot fix specific gaps like shared AI liability.

OPTION C | RECOMMENDED

Pursue clarity and enforcement in parallel

The evidence supports both being partially right. Pursue targeted legislative clarity, on AI content and shared accountability, while investing in enforcement capacity and public legal awareness within the current framework.

RECOMMENDATIONS

Clarity, enforcement and awareness, in parallel.

Each actor owns a specific, evidence-based move. The evidence does not force a choice between new law, better enforcement and public awareness; it calls for all three at once.

Government & regulators

- Invest in enforcement capacity — train police, prosecutors and courts through existing gender desks (the top ask, 74.4%).
- Close the deepfake gap — extend liability to those who supply enabling tools.
- Define statutory terms like "obscene" and "intimate".
- Sex-disaggregate complaints data at the ODPC.

Platforms & technology

- Increase transparency on data use and moderation (a top-three demand, 58.4%).
- Link pseudo-accounts so blocking one reaches the same abuser's others.
- Guarantee evidence windows before content is deleted.
- Move past passive AI disclosure to detection with real consequences.

Civil society & research

- Prioritise awareness and digital-safety education, the most demanded intervention.
- Reach the youngest bracket, under-sampled and most at risk.
- Coordinate to avoid fragmenting an under-resourced response.
- Build shared evidence so reform rests on triangulated data.



A response system survivors do not yet trust to act.

The evidence, from 219 survey respondents, six practitioners across case management, law, advocacy, regulation, training and platform research, and two focus groups of young women in Nairobi and Kitui, points to a consistent conclusion: online harm against young women in Kenya is routine, frequently dismissed, and met with a response system survivors do not trust to act.

Closing this gap does not require choosing between new law, better enforcement and public awareness. It requires pursuing all three, in parallel, with government, platforms and civil society each acting on the specific recommendations set out here.

METHODOLOGY NOTE

A concurrent mixed-methods study: a 219-respondent survey (16–35), six Key Informant Interviews and two Focus Group Discussions, conducted July to August 2026. All qualitative material was coded against a shared codebook of nine domains and 45 codes. A full account is available in the accompanying in-depth research report.



REFERENCES

Safe Digital Futures survey dataset, Sauti Salama, 2026 (n=219).

Key Informant Interviews: CREAW; independent legal practitioner; FIDA Kenya; ODPC; Nairobits; CIPIT, 2026.

Focus Group Discussions, Kitui & Nairobi, Sauti Salama, 2026.

UNFPA, Rapid Study on TFGBV in Kenya's Higher Learning Institutions.

UNFPA, Making All Spaces Safe: Technology-Facilitated Gender-Based Violence, 2020.

KICTANet, Addressing TFGBV: Kenya's Legal & Policy Landscape, Policy Brief No. 33.

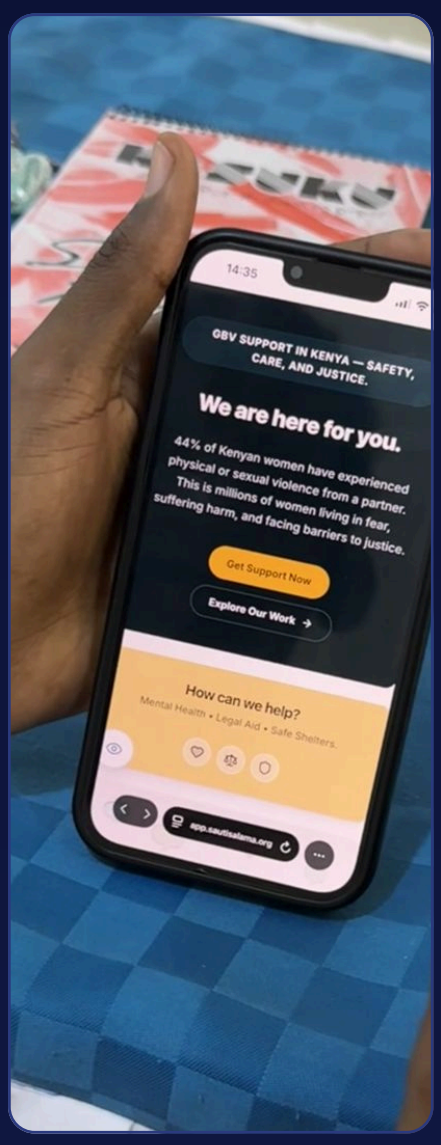
Republic of Kenya, Computer Misuse & Cybercrimes Act, 2018; Data Protection Act, 2019.

THE PLATFORM IN PRACTICE

Help is one tap away, on every screen.

Sauti Salama runs a mobile-first platform at app.sautisalama.org. It puts support ahead of information: the first screen offers help, and a Report Abuse button stays pinned to every page.

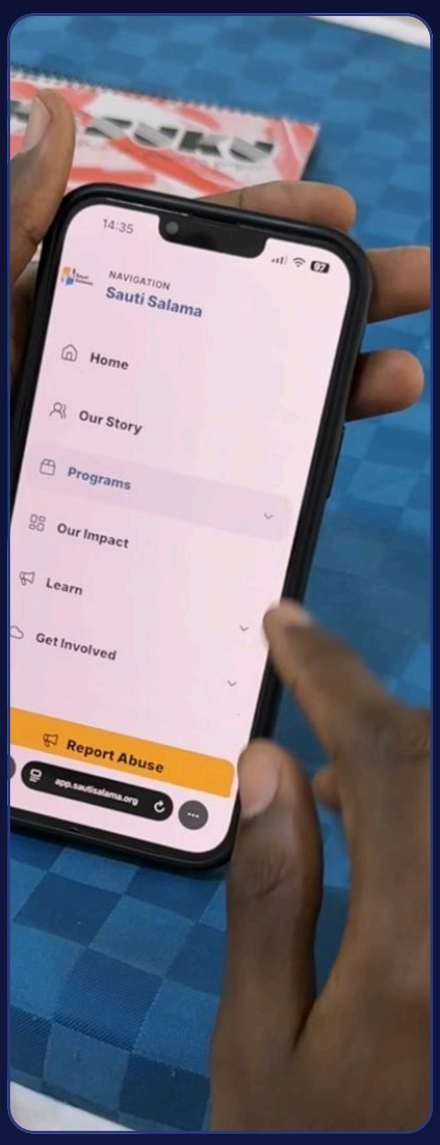
Survivors told us harm is routine and reporting feels pointless. A short, visible route to help is where rebuilding that trust starts.



01

Support first

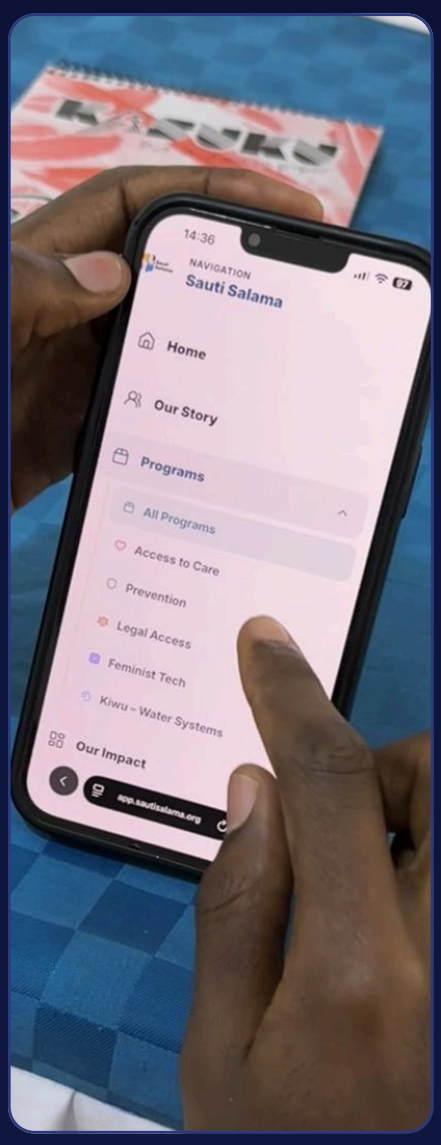
The home screen leads with Get Support Now: mental health, legal aid and safe shelters.



02

Clear navigation

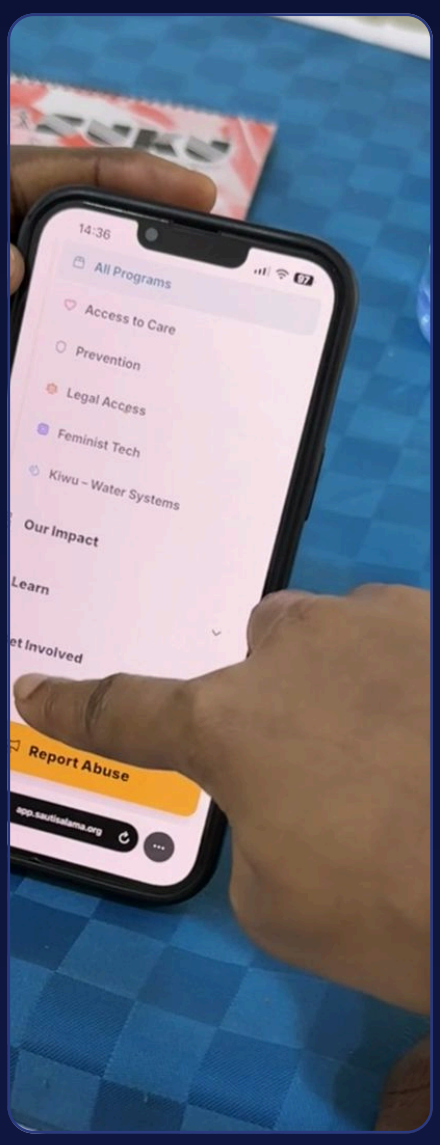
Home, Our Story, Programs, Our Impact, Learn and Get Involved, in one short menu.



03

Programmes in reach

Access to Care, Prevention, Legal Access, Feminist Tech and Kiwu water systems.



04

Report abuse

A pinned Report Abuse button is reachable from every page.

ABOUT THESE SCREENS

Stills from a walkthrough of app.sautisalama.org on a mobile phone.

A response system survivors do not yet trust to act.

The evidence, from 219 survey respondents, six practitioners across case management, law, advocacy, regulation, training and platform research, and two focus groups of young women in Nairobi and Kitui, points to a consistent conclusion: online harm against young women in Kenya is routine, frequently dismissed, and met with a response system survivors do not trust to act.

Closing this gap does not require choosing between new law, better enforcement and public awareness. It requires pursuing all three, in parallel, with government, platforms and civil society each acting on the specific recommendations set out here.

METHODOLOGY NOTE

A concurrent mixed-methods study: a 219-respondent survey (16–35), six Key Informant Interviews and two Focus Group Discussions, conducted July to August 2026. All qualitative material was coded against a shared codebook of nine domains and 45 codes. A full account is available in the accompanying in-depth research report.



REFERENCES

Safe Digital Futures survey dataset, Sauti Salama, 2026 (n=219).

Key Informant Interviews: CREAW; independent legal practitioner; FIDA Kenya; ODPC; Nairobits; CIPIT, 2026.

Focus Group Discussions, Kitui & Nairobi, Sauti Salama, 2026.

UNFPA, Rapid Study on TFGBV in Kenya's Higher Learning Institutions.

UNFPA, Making All Spaces Safe: Technology-Facilitated Gender-Based Violence, 2020.

KICTANet, Addressing TFGBV: Kenya's Legal & Policy Landscape, Policy Brief No. 33.

Republic of Kenya, Computer Misuse & Cybercrimes Act, 2018; Data Protection Act, 2019.

Sauti Salama