PATHWAYS OF PROMISE KENYA | RESEARCH & PRACTICE SERIES
Discussion Paper No. 01

Beyond the Donation: Digital Philanthropy, Artificial Intelligence and the Protection of Children and Families Affected by Incarceration in Kenya

Elizabeth Wambui Mumbi
Founder, Pathways of Promise Kenya, Nairobi
October 2026 | Version 1.0

Publication status. This is a conceptual, practice-oriented discussion paper. It has not been peer-reviewed and does not report findings from an empirical study. It has not been reviewed by a legal practitioner and is not legal advice; the legislation and guidance it summarises should be checked against current texts before operational reliance.

Correspondence. info@pathwaysofpromisekenya.org | https://pathwaysofpromisekenya.org

Suggested citation. Mumbi, E. W. (2026). *Beyond the donation: Digital philanthropy, artificial intelligence and the protection of children and families affected by incarceration in Kenya* (Research & Practice Series, Discussion Paper No. 01). Pathways of Promise Kenya. https://pathwaysofpromisekenya.org

Author's note and positionality

I founded Pathways of Promise Kenya and lead it. The paper uses the organisation as an illustrative case, and I have written it with that relationship in view: I am not an independent observer, and Section 7 describes plans and commitments, not an evaluated programme. The paper grew out of informal visits to a women's prison, where I saw young children living with their mothers and mothers who were struggling with their mental health and with understanding their legal position. Those observations are not research data and are not reported as findings. They are the reason I became concerned with how an organisation like mine should ask for support, and handle information, without exposing the people it exists to help. Applying the paper's own standard, I have not named the facility or described any individual.

Abstract

Digital tools and artificial intelligence (AI) are changing how philanthropic organisations raise funds, communicate with supporters, coordinate programmes and report on impact. For small Kenyan non-profits these tools can widen reach and ease administration. They also create risks for the people whose circumstances motivate giving: photographs, stories, family relationships and locations can be copied, combined with other details, and reused far beyond their original purpose. This discussion paper examines those risks with particular attention to children affected by parental incarceration and their mothers, a group whose association with a parent's imprisonment can expose them to stigma and whose capacity to consent is shaped by custody. Drawing on Kenyan legislation and regulatory guidance, international child-rights standards, scholarship on the ethics of representation, and guidance on AI, the paper proposes a safeguarding-centred framework of seven pillars: data governance, privacy by design, secure information management, ethical storytelling and consent, responsible AI use, donor accountability without beneficiary exposure, and incident response with continuous improvement. It applies the framework to Pathways of Promise Kenya, a new organisation, as an illustrative case. The framework has not been implemented or evaluated. The paper argues that digital capability should be judged not only by fundraising reach or efficiency, but by an organisation's ability to prevent foreseeable harm, keep confidences and remain accountable to the people whose experiences inform its work.

Keywords: digital philanthropy; data protection; safeguarding; children of incarcerated parents; ethical storytelling; artificial intelligence; Kenya

Contents

1. Introduction 3

2. Digital Philanthropy and the Ethics of Representation 4

3. Children and Families Affected by Incarceration: A Distinct Context 6

4. The Kenyan Legal and Regulatory Framework 7

5. Artificial Intelligence: Opportunities, Risks and Responsible Adoption 9

6. A Safeguarding-Centred Framework for Digital Philanthropy 11

7. Pathways of Promise Kenya as an Illustrative Case 13

8. Recommendations 15

9. Limitations and Future Research 16

10. Conclusion 16

References 17

1. Introduction

Digital technologies are reshaping how philanthropic organisations mobilise resources, communicate with donors, coordinate programmes and demonstrate impact. Online donation platforms, mobile payments, websites, social media, cloud storage and AI offer new ways to reach supporters and organise information. For small and emerging non-profits, these tools can be especially attractive, because they promise wider access to donors without the resources of a large institution.

Digitisation also brings a responsibility that receives less attention: protecting the personal information, dignity and safety of the people whose needs motivate giving. The risks go beyond hacking. Information may be collected unnecessarily, kept too long, sent to the wrong recipient or repurposed in ways no one anticipated. A photograph or story published to attract donations can be copied and separated from its context, and removing the original post does not remove the copies. Details that are harmless alone can identify a person when combined.

These risks are acute for children affected by parental incarceration. A child's association with an imprisoned mother may be revealed without the child's name appearing anywhere, through a location, an age, a caption or a uniform in the background. For a mother in custody, her legal circumstances are private, and her ability to say no to a request from the people providing her with help is limited. Kenya's Constitution and Data Protection Act, and international instruments on children's rights and on women prisoners, all bear on these questions, yet small organisations rarely have the capacity to translate them into practice.

This paper argues that protecting personal data, dignity and safety should be treated as a core part of responsible digital philanthropy, designed in from the start, and not an administrative matter addressed after fundraising and programme systems are in place. Digital capability should include the ability to assess risk, limit collection, explain decisions and remain accountable to the people affected.

1.1 Scope, objectives and questions

The paper focuses on children affected by parental incarceration, including children living with their mothers in prison, and on their mothers. Survivors of gender-based violence and trafficking face related but distinct digital risks; they are mentioned in Section 3.5 but the framework is not extended to them without adaptation. The paper has three objectives: to examine the opportunities and risks of digital tools and AI for small philanthropic organisations; to set out the Kenyan legal and international rights context; and to propose an initial framework for digital fundraising, beneficiary information, administration and AI use. It asks:

1. How can digital tools and AI strengthen fundraising, capacity and accountability without unnecessarily increasing risk to the people receiving support?
2. What privacy, safeguarding and ethical risks arise when organisations collect, store, process or publicise information about children and families affected by incarceration?
3. What practical principles and safeguards can small and emerging organisations adopt to govern digital philanthropy responsibly?

1.2 Approach and limitations

The paper is a conceptual, practice-oriented discussion based on a desk review of selected Kenyan legislation and regulatory guidance, academic and practitioner literature on digital philanthropy and the representation of suffering, and international publications on children's rights, AI and technology-facilitated gender-based violence. It reports no interviews, survey or evaluation. Pathways of Promise Kenya is used as an illustrative case (Section 7), and the author's relationship to it is stated above. The proposed framework is an initial contribution to organisational learning and a basis for consultation and future research (Section 9).

2. Digital Philanthropy and the Ethics of Representation

2.1 What digital philanthropy involves

Digital philanthropy is the use of digital technologies to facilitate or change charitable giving, fundraising, donor engagement, programme coordination and the relationship between organisations and communities. It includes online donation platforms, mobile payments, crowdfunding, email, social media, cloud-based records and AI applications. Digitisation, such as replacing paper records or cash with electronic ones, differs from digital transformation, in which technology becomes embedded in how an organisation works. Research on non-profits stresses the role of leadership, collaboration, usability and organisational learning in making digital transformation serve social purposes (Jong & Ganzaroli, 2024). A new donation platform does not by itself improve accountability or safeguarding, and moving records to the cloud makes them easier to retrieve while creating new duties about access, security and retention.

2.2 Giving and fundraising in Kenya

Kenyan giving draws on long traditions of community support, including Harambee. Digital channels can extend those practices to contributors beyond a person's immediate network. The Kenya study in the Digital for Good series examined emerging approaches such as crowdfunding and workplace giving (Indiana University Lilly Family School of Philanthropy & East Africa Philanthropy Network, 2022), and Kusimba's (2025) study of M-Changa shows how online fundraising is embedded in networks of family, friendship, care and obligation, rather than being a purely technical transaction. Donors give because they trust a fundraiser or recognise a cause. Online access does not guarantee reliable income, and a payment channel does not show that a campaign is legitimate or that funds were used well. Organisations still need sound financial records and credible accounts of activity.

Financial transparency is not the same as unrestricted access to beneficiaries' personal information. Donors need meaningful accountability, but ordinarily do not need identifiable case files, children's names or sensitive family histories. Budgets, expenditure summaries, aggregate indicators and distribution records can show how funds were used without exposing individuals.

2.3 Representation, storytelling and the digital layer

Long before digital fundraising, scholars and practitioners questioned how charities portray the people they serve. Dogra (2012) examined how international NGOs represent global poverty and the stereotyped, depoliticised images that recur in their communications, and Chouliaraki (2013) analysed how humanitarian appeals have changed in the way they address audiences and depict suffering. Sector codes responded. The Dóchas Code of Conduct on Images and Messages (Dóchas, 2007) commits signatories to respect for dignity, to avoid stereotyping and sensationalism, and to use images and case studies with the understanding and permission of the subjects or their parents or guardians. UNICEF's (n.d.) ethical reporting guidelines go further for children, placing each child's best interests above advocacy for children's issues and cautioning against publication that could expose a child or relatives to harm even where identities are obscured.

Digital media change the stakes. Material published online can be copied, indexed, forwarded and combined with other information, and the organisation cannot fully control what happens next. Before publishing, an organisation should therefore ask who has authority to publish information about a person, whether that person understands how far it may travel, whether it could expose them or their relatives, and whether a less intrusive alternative would serve the same purpose. Ethical storytelling does not require silence. It requires distinguishing between explaining a problem and identifying the people affected by it. Needs, the type of assistance, budgets and aggregate results can be communicated without routinely publishing names or family histories, and non-identifying images, clearly labelled illustrations and anonymised examples can convey context.

2.4 Information management and unequal capacity

Spreadsheets, donor-management systems, accounting software, cloud storage and programme databases can reduce duplication and speed reporting. They can also concentrate records and make them easy to copy. Overly permissive links, compromised accounts, personal-device storage and access that outlasts a person's role are everyday sources of exposure, and external providers may process data under terms an organisation has not read. Financial records and confidential programme records serve different purposes and should be kept apart with access tied to legitimate roles.

Organisations also differ in connectivity, funds, skills and training. Subscriptions, payment processing and cybersecurity are real costs for small non-profits, and dependence on external platforms exposes them to changes in price, terms and availability. Not everyone has reliable internet, a device or a bank account, so an exclusively digital strategy can exclude people it means to reach. Smaller organisations often gain stronger protection from clear procedures, data minimisation and well-configured existing tools than from a complex system they cannot maintain.

3. Children and Families Affected by Incarceration: A Distinct Context

3.1 Digital vulnerability

Digital vulnerability is not simply a lack of technology or digital literacy. In philanthropic settings it arises from the interaction of a person's circumstances, the information held about them, the systems through which it travels, and unequal power over how it is used. A child has little say over whether an organisation publishes a photograph. The central question is therefore not only whether an organisation has permission to collect or publish information, but whether the information is necessary, who may access it, how it might be combined with other information, what disclosure could lead to, and whether safeguards are in place.

3.2 Identification and cumulative disclosure

Personal information includes more than names and contact details: photographs, locations, family relationships, health circumstances, school details and legal circumstances all count, and information that does not identify a person alone may do so in combination. A report may omit a child's name yet identify an institution, an age range and a family relationship. A blurred face may still be recognisable from clothing, surroundings or a caption. The ODPC's (2025) guidance on children's data emphasises minimisation, confidentiality, privacy by design and assessment of risks to children's rights.

This cumulative risk is greatest in closely connected communities, where relatives and neighbours may recognise a child from limited clues. It also arises over time: a confidential programme record may later be copied into a report, a presentation, a social media post or an AI tool, and each new use changes the audience and the consequences. Data minimisation therefore has to apply throughout the information lifecycle, not only at collection.

3.3 Rights standards for children with incarcerated mothers

A body of international and regional standards addresses children whose mothers are imprisoned. Article 16 of the Convention on the Rights of the Child (United Nations General Assembly, 1989) protects children against arbitrary or unlawful interference with privacy, and Article 10 of the African Charter on the Rights and Welfare of the Child (Organisation of African Unity, 1990) likewise protects privacy. Article 30 of the African Charter makes specific provision for children of imprisoned mothers. The Bangkok Rules (United Nations General Assembly, 2010) require that decisions about children staying with their mothers in prison be based on the child's best interests, provide that such children shall never be treated as prisoners (Rule 49), and call for ongoing health care and developmental monitoring (Rule 51). The Committee on the Rights of the Child (2011) devoted a Day of General Discussion to children of incarcerated parents, and its General Comment No. 25 (2021) applies children's rights, including privacy and best interests, to the digital environment.

None of these instruments addresses digital fundraising directly. Together, however, they establish that the dignity, privacy and best interests of children in this situation are protected rights, and that how an organisation represents these children in fundraising is within their scope. They also frame the child as a rights-holder, not a symbol of need.

3.4 Advocacy, consent and custody

Children affected by parental incarceration illustrate the tension between advocacy and privacy. A parent's imprisonment may explain why a programme exists, but linking an identifiable child to it can invite stigma, bullying or unwanted scrutiny. Photographs taken in an institution can reveal the child, the mother or the place through uniforms, signs or captions. This does not mean these children should be absent from public discussion. Advocacy can report the number of children supported, the types of assistance and the resources required without publishing identifiable images or family histories.

Consent needs particular care. Kenya's Data Protection Act generally requires parental or guardian consent to process a child's data, together with protection of the child's rights and best interests, subject to the Act's provisions and exceptions (Republic of Kenya, 2019, s. 33). Consent is not a universal permission: best interests and foreseeable harm remain the test. For mothers in custody, voluntariness is harder to establish. A woman who depends on an organisation, and through it on access to supplies or support, may feel unable to refuse a photograph or testimony even if no one pressures her. Consent to receive assistance must be kept separate from consent to be used for publicity, and assistance must never depend on agreeing to publicity. In a custodial setting, the safer default is not to seek publicity consent at all and to use non-identifying material; any exception would need institutional permission and consent that is informed, specific, independent of aid and revocable. Ethical storytelling also respects agency: the people concerned are not fundraising assets whose value rests on the emotional force of their suffering.

3.5 Other groups

Survivors of gender-based violence and trafficking face related risks, including technology-facilitated abuse such as doxxing, image-based abuse and harassment, which a joint technical brief by UNFPA, UNICEF and Save the Children examines (UNFPA et al., 2025). The risks and appropriate protections differ across groups and should not be treated as interchangeable. This paper does not extend its framework to them; organisations serving them should adapt it with specialist advice.

4. The Kenyan Legal and Regulatory Framework

This section summarises provisions relevant to a small organisation handling information about children and families. It is not legal advice, and the provisions and guidance should be checked against current texts.

4.1 Constitutional foundations

Article 31 of the Constitution protects privacy, including against unnecessary disclosure of information relating to family or private affairs. Article 53 sets out children's rights and provides that a child's best interests are of paramount importance in every matter concerning the child (Republic of Kenya, 2010). A legitimate purpose for helping a family does not automatically justify making the same information available to donors or the public.

4.2 The Data Protection Act, 2019

The Act is the principal statute on personal data. Processing covers collection, recording, storage, use, disclosure and deletion, so a non-profit has duties through ordinary programme administration, on paper or digitally. Section 25 sets out the principles: lawful, fair and transparent processing; collection for explicit and legitimate purposes; limiting data to what is necessary; accuracy; appropriate retention; and safeguards. Section 26 gives data subjects rights, including to be informed, to access their data, to object, and to request correction or deletion in defined circumstances (Republic of Kenya, 2019).

The Act's definition of sensitive personal data includes family details, including the names of a person's children and parents (Republic of Kenya, 2019, s. 2). This matters directly here: a record that names a mother and her child is likely to attract the additional requirements the Act places on sensitive personal data. Even where a record falls outside a statutory category, its disclosure may still pose serious practical and safeguarding risks.

4.3 Children's data, the Children Act and registration

Section 33 addresses the processing of children's personal data, generally requiring parental or guardian consent and processing that protects and advances the child's rights and best interests. It includes an exception for certain organisations exclusively providing counselling or child-protection services, so its application to any given non-profit depends on the facts and the law (Republic of Kenya, 2019, s. 33). The Children Act, 2022 reinforces the best-interests principle (Republic of Kenya, 2022). The ODPC's (2025) guidance on children's data addresses lawful purposes, sensitive data, privacy by design, high-risk processing and registration, and states that entities processing children's data are required to register as data controllers or processors.

The Registration Regulations (Republic of Kenya, 2021b) provide a threshold exemption for small entities, framed by annual turnover or revenue and number of employees, but the exemption does not apply to every kind of processing. A small organisation working with children should confirm its position against the Regulations and current ODPC guidance instead of assuming it is exempt.

4.4 Impact assessment and privacy by design

Section 31 requires a data protection impact assessment (DPIA) before processing likely to result in a high risk to data subjects' rights and freedoms, and the General Regulations (Republic of Kenya, 2021a) contain provisions on data protection by design or default and on impact assessment. The ODPC (2024) has issued a guidance note on DPIAs. Whether a formal DPIA is legally required depends on the facts, but a short risk review before building a central database of sensitive case histories, collecting children's location or biometric data, or introducing extensive monitoring is good practice either way. Privacy by design means deciding in advance which fields are necessary, who needs access, how long identifiable data will be kept and whether donor reporting can be done with aggregate information.

4.5 Security and breach response

The Act requires appropriate technical and organisational measures to protect personal data. Section 43 requires a data controller to notify the Data Commissioner of a qualifying breach that creates a real risk of harm without delay and within seventy-two hours of becoming aware of it, with related provisions on processors and affected individuals (Republic of Kenya, 2019, ss. 41–43). Because the response depends on the incident, organisations should decide before one occurs who receives reports, who assesses risk, how further disclosure is contained and how notification duties are determined. Practical controls include sensible account permissions, strong authentication, secure backups, protected devices, controlled file sharing and prompt removal of access when roles change. Guidance written for Kenyan civil society covers data maps, privacy policies, vendor management, impact assessments and incident response (Amnesty International Kenya & Data Privacy and Governance Society of Kenya, 2025), and a 2026 manual adds records of processing, data classification and cross-border transfers (Ndede et al., 2026).

4.6 Providers, cross-border data and automated decisions

Donation services, cloud platforms, email and AI tools may process information outside an organisation's own systems. Before adopting one, an organisation should understand what it collects, how it processes and retains data, whom it shares data with and what cross-border transfer implications arise under Kenyan law. The Act also addresses decisions based solely on automated processing that produce legal effects or significantly affect a person, subject to exceptions and safeguards (Republic of Kenya, 2019, s. 35). That is relevant if AI were used to decide eligibility for support; it does not mean every use of generative AI for routine drafting is covered.

4.7 Beyond compliance

Legal compliance is necessary but does not settle every ethical question. A publication may satisfy formal requirements and still reveal more than necessary; a person may consent to a use without foreseeing how permanent it will be; a secure database may hold information an organisation has no good reason to keep. General Comment No. 25 (Committee on the Rights of the Child, 2021) treats privacy as central to children's dignity and safety in the digital environment. Responsible practice asks whether processing is necessary, proportionate and consistent with the mission, and does not make publicity a condition of assistance.

5. Artificial Intelligence: Opportunities, Risks and Responsible Adoption

5.1 Beyond the simple debate

The question for a non-profit is not whether to embrace or reject AI, but which uses are appropriate. The risks depend on the tool, the data supplied, the purpose and the safeguards. UNESCO's (2021) Recommendation on the Ethics of Artificial Intelligence identifies human rights, proportionality, privacy, accountability and human oversight as key considerations; UNICEF's (2025) guidance on AI and children adds child-rights concerns including safety, fairness and best interests; and the National Institute of Standards and Technology offers risk-management resources, including a profile for generative AI (National Institute of Standards and Technology [NIST], 2023; Autio et al., 2024).

5.2 Potential benefits for small non-profits

AI may help draft general correspondence, organise funding calendars, summarise public reports, translate non-confidential material, outline report structures and prepare general educational resources. It may help structure a grant proposal around a funder's published requirements, provided staff verify the content and ensure the final submission accurately reflects the organisation's work and capacity. It can also assist analysis of appropriately aggregated programme information, though results depend on data quality and how categories were defined, and a pattern is not proof of cause or effectiveness. Such uses save staff time but do not guarantee better performance; their value should be tested in practice.

5.3 Confidentiality, accuracy and fabricated content

A central risk is entering confidential information into AI tools without understanding the provider's data practices. Uploading a case report, pasting identifiable beneficiary details into a prompt or asking a system to turn sensitive notes into a fundraising story can expose information beyond the organisation's control. Terms vary by provider and configuration, and it would be wrong to assume every service uses all inputs for training or makes them public. The sound approach is to understand the terms and to minimise personal information supplied. Many tasks can be done with general descriptions, fictional examples or aggregate figures.

Generative AI can state falsehoods confidently, fabricate citations and omit key context (Autio et al., 2024). Translations may change legal or safeguarding meaning, and outputs may reproduce stereotypes that portray communities as passive or helpless. Claims about legislation, funding and outcomes therefore need checking against sources and records. Synthetic images may sometimes avoid exposing real beneficiaries if they are honestly labelled as illustrations. Invented testimonials, fabricated distribution photographs or AI-generated accounts presented as authentic are incompatible with credible philanthropy and dishonour the people they claim to represent.

5.4 Human oversight and dependency

AI should not replace human judgement in safeguarding decisions, assessments of abuse disclosures, decisions on eligibility or other consequential matters. Responsibility stays with the organisation and the people authorised to decide. External AI also creates dependency on providers whose prices, terms and products may change. At organisational level, digital sovereignty means keeping real agency over the purposes and information behind one's work, not building one's own AI. Kenya's National AI Strategy 2025–2030 identifies infrastructure, data, skills, governance, ethics, equity and inclusion as elements of national AI development (Ministry of Information, Communications and the Digital Economy, 2025), themes that reinforce the need for informed, locally grounded adoption.

5.5 A risk-based approach

Table 1 is an internal planning aid, not a statutory classification. The assessment depends on the tool, the information used and the consequences of the output. Where risks are unnecessary or cannot be controlled, deciding not to use AI is a legitimate result of good governance.

Table 1. Initial risk assessment of proposed AI uses

Proposed use	Initial assessment	Suggested approach
Drafting general public information from public sources	Lower risk	Permit with factual and editorial review.

Proposed use	Initial assessment	Suggested approach
Creating non-confidential planning templates	Lower risk	Permit without personal data; review usefulness.
Translating general information	Low to moderate risk	Review carefully where legal or safeguarding meaning matters.
Analysing aggregated programme totals	Moderate risk	Check data quality and whether individuals could be re-identified.
Uploading identifiable child or survivor case files to an external AI tool	High risk	Do not proceed without a documented legal, privacy and security assessment; prefer alternatives.
Using AI to decide eligibility or assess abuse disclosures	High risk	Do not delegate the decision; keep human assessment.
Presenting synthetic content as authentic evidence or testimony	Unacceptable	Do not fabricate or misrepresent programme evidence.

6. A Safeguarding-Centred Framework for Digital Philanthropy

6.1 Purpose and status

Safeguarding cannot be reduced to cybersecurity. It involves organisational choices about collection, consent, publication, AI use, access, retention and accountability. The framework below integrates these across the digital lifecycle. It draws on Kenya's legal framework, ODPC guidance, international child-rights and AI principles, and established risk management, including the NIST AI Risk Management Framework's four functions of Govern, Map, Measure and Manage (NIST, 2023). It is an initial conceptual model and has not been validated through implementation or evaluation.

6.2 Foundational principles

Human dignity and rights. Technology should serve legitimate purposes without reducing people to data points or fundraising assets; children's best interests stay central. **Data minimisation.** Collect only what a defined, legitimate purpose needs. **Purpose limitation.** Information gathered for delivery is not automatically reused for publicity, research, donor reporting or AI. **Proportionate safeguards.** Controls reflect sensitivity and consequence; a small organisation can begin with clear procedures and well-configured tools. **Human accountability.** Digital systems and AI assist decisions but do not remove organisational responsibility. **Accountability to people represented.** People whose information is processed receive explanations and routes to raise concerns, and never have to accept publicity as a condition of help.

6.3 Seven pillars

- **Pillar 1: Data governance and institutional accountability.** Assign responsibility; identify legal obligations, information categories and approved systems; set procedures for reviewing new processing, answering requests and handling incidents.
- **Pillar 2: Privacy by design and minimisation.** Fix the purpose and necessary data before building forms, databases or workflows; separate distinct purposes; use aggregate or non-identifying information wherever it suffices.

- **Pillar 3: Secure information management.** Use access controls, account security, secure sharing and backups; separate sensitive programme records from donor and public information; set retention and disposal rules.
- **Pillar 4: Ethical storytelling and consent.** Assess the purpose and risks of any photograph or story before publication; obtain legally appropriate permission; respect best interests; prefer less intrusive alternatives. Consent does not remove the duty to assess foreseeable harm.
- **Pillar 5: Responsible AI use.** Approve defined use cases; minimise data supplied; assess providers and terms; verify outputs; prohibit fabricated evidence; keep human oversight of consequential decisions.
- **Pillar 6: Donor accountability without beneficiary exposure.** Show how resources were used through financial documents, aggregate indicators and distribution records, not unrestricted access to personal records.
- **Pillar 7: Incident response and continuous improvement.** Set clear routes to report suspected disclosure, contain risk, assess notification duties, support affected people and learn from incidents and near misses.

6.4 Keeping functions apart

A practical way to apply Pillars 2, 3 and 6 is to treat four functions as distinct, with different audiences and rules (Table 2).

Table 2. Information functions and the rules that should govern them

Function	Typical content	Access and disclosure rule
Financial records	Donations, expenditure, receipts, bank records	Finance role and auditors; funders receive summaries and supporting documents without beneficiary identifiers.
Programme records	Needs verification, distribution lists, health referrals, safeguarding notes	Named staff with a defined role; confidential; never used for publicity; shared outward only in aggregate.
Public communications	Website, social media, reports, appeals	Aggregate figures, budgets and non-identifying or clearly illustrative material; each item reviewed before publication.
Research data	Interviews, surveys, analysis datasets	Collected only with separate ethical review, consent and permissions; never a by-product of programme access.

6.5 The digital safeguarding lifecycle

Table 3. Safeguarding questions and actions across the information lifecycle

Stage	Key question	Safeguarding action
Planning	Why is the information or tool needed?	Define the purpose and consider less intrusive alternatives.
Collection	What information is necessary?	Minimise data and explain its use.
Storage and access	Who needs access and why?	Configure permissions, security and retention rules.

Stage	Key question	Safeguarding action
Use and analysis	Is this use consistent with the defined purpose?	Review sharing and AI uses; verify outputs.
Publication	Could disclosure expose someone to harm?	Assess identification, necessity, audience, permission and consequences.
Retention and disposal	Is identifiable information still necessary?	Apply retention rules; delete or anonymise securely.
Review and response	What if practice fails or circumstances change?	Report incidents, assess impact and improve procedures.

6.6 Phased implementation

An emerging organisation can implement the framework in stages. The first stage establishes its legal position, names a responsible person, inventories the main categories of information, adopts basic confidentiality and publication procedures, and gives staff and volunteers practical instructions. The second reviews tools and information flows, configures access, documents retention and incident response, and assesses higher-risk processing. The third monitors compliance, reviews AI uses and seeks specialist advice. A later stage can document and share lessons once practices have been implemented and assessed. A policy alone does not prove that information is handled properly; implementation and review are what count.

7. Pathways of Promise Kenya as an Illustrative Case

7.1 Context and status

Pathways of Promise Kenya was established in October 2024 and focuses on children affected by parental incarceration, including children living with their mothers in prison. It is a small, founder-led and founder-funded organisation that is planning its first programme, a pilot providing essential supplies and related support, and it has had early engagement with a women’s prison. It is used here to show how the questions in this paper arise before an organisation has built extensive digital infrastructure. This section describes proposed practice, not implemented or evaluated practice. Following the principle in Section 3.2, the facility is not named, and the paper does not report cohort details that could help identify individuals.

7.2 Fundraising without exposure

Pathways can explain the need for supplies, publish transparent budgets, report distributions and use aggregate information to demonstrate activity. It does not need to publish identifiable photographs or detailed histories of children and mothers to show why the work matters. Before using any photograph or account, it should ask whether the item is necessary, whether direct or indirect identification is possible, whether the legal basis and permissions are in place, and whether publication could cause foreseeable harm. Given the custodial setting (Section 3.4), the default is non-identifying material. Donor requests should be assessed against legitimate purpose and safeguarding; donor preference alone should not override privacy.

7.3 Applying the lifecycle

At the needs-identification stage, Pathways should collect only what is necessary and agree with the prison administration what may be shared. Internal records should separate distribution information from confidential personal circumstances and restrict access. Public communications should be checked for photographs, captions, locations and contextual clues. Donor reports should rest on expenditure, supplies, activities and evidenced outcomes, and retention rules should prevent indefinite storage of identifiable records. Each tool, from the website to the donation channel, should have a defined purpose, a responsible user and safeguards matched to the information involved, and providers' terms and security should be assessed before personal data is processed through them.

7.4 AI and governance

Pathways could begin with AI-assisted tasks that need no confidential beneficiary information, such as drafting general programme descriptions, organising a funding calendar, summarising published policy or preparing non-confidential templates. AI should not be used to invent beneficiary stories, create misleading images or fabricate evidence, and identifiable child records should not be put into general-purpose AI services for convenience. A short AI-use policy should list approved tools and tasks, prohibited uses, review requirements and a route for assessing higher-risk proposals, and legal claims, citations and programme reports should be verified before publication.

Governance should clarify who may collect information, access programme records, publish website content, communicate with donors and approve AI use. Arrangements with the prison administration and other partners should specify what information is needed, what may be shared, for what purpose and under which safeguards; responsibilities should not be assumed where children's information is involved. Staff and volunteers should know how to raise a concern promptly.

7.5 Immediate priorities

The following are priorities for the organisation. They are recommended actions, not completed ones, and their design should reflect Pathways' actual systems, legal obligations, resources and programme activities.

- Confirm its registration position with the Office of the Data Protection Commissioner and register where required.
- Designate a person responsible for data protection.
- Map the information it collects and the services that process it.
- Adopt core procedures on confidentiality, consent, access, retention, publication and incident response, and keep public reporting separate from confidential programme records.
- Adopt a short AI-use policy.
- Agree in writing with the prison administration what information is needed, what may be shared and why.
- Train anyone who handles information, and review arrangements as activities develop.

7.6 What an internal case can and cannot show

Because the author leads the organisation, the case is illustrative and not independent. It shows how the framework's questions arise in a real, resource-constrained setting; it does not show that the framework works. Any future account should distinguish implemented practice from observed results and recommendations, and should ideally be assessed by someone outside the organisation. Pathways illustrates that choices made early about fundraising, collection, reporting and AI can either set responsible boundaries or form habits that are hard to change later.

8. Recommendations

8.1 For civil society organisations

- **Make data protection a governance responsibility.** Name who coordinates compliance, inventory data, verify ODPC registration and assessment requirements, and set procedures for access, retention, data-subject requests and incidents.
- **Minimise collection and circulation.** Collect only what a defined purpose needs; separate programme, donor, financial and public functions; do not keep identifiable information without a continuing need.
- **Adopt ethical fundraising and storytelling.** Do not make identifiable photographs or personal histories the default evidence of need; assess necessity and harm before publication.
- **Govern AI use.** Approve defined tasks, keep sensitive personal data out of unassessed systems, verify outputs and never fabricate evidence.
- **Prepare for incidents.** Provide reporting routes, a response procedure and training, and learn from near misses.

8.2 For funders

Funders should recognise data protection, cybersecurity and responsible AI governance as legitimate organisational costs. Reporting requirements should be proportionate and should not routinely demand identifiable beneficiary information where aggregate or independently verified evidence will do. Funding criteria should value safeguarding capacity and support training and access to specialist advice.

8.3 For technology providers

Providers should make privacy and security settings understandable, explain data processing and retention clearly, and offer accessible ways to restrict access or delete information. AI providers should state the terms that apply to submitted data and the limits of their systems, and tools aimed at non-profits should support safe use by organisations with limited technical capacity.

8.4 For regulators and policymakers

Public institutions should keep providing accessible guidance on data protection, children's rights, AI and technology-facilitated violence, and help small organisations identify when registration, impact assessment or other safeguards apply. Clearer coordination among institutions would help in sensitive cases involving children in custody.

8.5 For researchers and civil society networks

Research should examine how non-profits manage consent, whether donor requirements encourage unnecessary disclosure, how organisations assess external platforms and what hinders responsible AI adoption. Networks can support peer learning through model policies, training and practical guidance.

9. Limitations and Future Research

This is a conceptual, practice-oriented paper based on selected legislation, guidance, scholarship and international publications. It reports no interviews, surveys or evaluation. Pathways is one small organisation in a particular legal and institutional setting and is not representative of all non-profits; the author's relationship to it is disclosed above. The framework has not been tested, and the risks discussed are potential risks, not claims that any incident has occurred or that technology invariably causes harm. The literature drawn on is selective, and legal provisions, guidance and provider terms should be rechecked, preferably with a Kenyan advocate, before operational decisions.

Future work could document how an organisation implements data-governance procedures, compare practice across Kenyan non-profits, examine how donor reporting requirements shape disclosure, and study how organisations assess AI tools. It should distinguish policy adoption from evidence that implementation improves practice or reduces harm. Research involving children, incarcerated mothers or confidential records needs its own ethical review, permissions and safeguards; access to a programme is not authorisation to research it.

10. Conclusion

Digital technologies and AI give philanthropic organisations real opportunities to raise resources, communicate and strengthen administration. The same information that enables these activities can reveal sensitive circumstances, and poorly governed AI can add risks to confidentiality, accuracy and representation. This paper has argued that protecting personal data, dignity and safety is central to responsible digital philanthropy, and has proposed a framework that joins data governance, minimisation, secure management, ethical storytelling, responsible AI, donor accountability and continuous improvement.

For children affected by parental incarceration, the lesson is concrete. Information needed to deliver support is different from information needed to raise funds or report on results, and an organisation can explain genuine need and show responsible use of resources without publishing children's identities or family histories. The framework remains a proposal that needs implementation, documentation and independent evaluation. Its central principle is clear: responsible digital philanthropy should be measured not only by money raised or the speed of adopting technology, but by the ability to protect the people whose information it holds and whose circumstances inform its work.

> *People who receive philanthropic support are not subjects of reports, photographs, databases or AI-generated outputs. They are rights-holders whose dignity, privacy and agency must stay central to the systems built in their name.*

References

African Union (Organisation of African Unity). (1990). *African Charter on the Rights and Welfare of the Child* (OAU Doc. CAB/LEG/24.9/49).

Amnesty International Kenya, & Data Privacy and Governance Society of Kenya. (2025). *Data protection guidelines for civil society organisations*. https://www.amnestykenya.org/wp-content/uploads/2025/10/CSO-Data-Protection-Guidelines-Final.pdf

Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

Chouliaraki, L. (2013). *The ironic spectator: Solidarity in the age of post-humanitarianism*. Polity Press.

Committee on the Rights of the Child. (2011). *Report and recommendations of the Day of General Discussion on children of incarcerated parents* (30 September 2011). United Nations.

Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment* (CRC/C/GC/25). United Nations.

Dóchas. (2007). *Code of conduct on images and messages*. Dóchas. https://www.dochas.ie

Dogra, N. (2012). *Representations of global poverty: Aid, development and international NGOs*. I.B. Tauris.

Indiana University Lilly Family School of Philanthropy, & East Africa Philanthropy Network. (2022). *Digital for good: A global study on emerging ways of giving—Kenya*. https://globalindices.iupui.edu/additional-research/digital-for-good/kenya.html

Jong, C. L. K., & Ganzaroli, A. (2024). Managing digital transformation for social good in non-profit organizations: The case of The Felix Project Zeroing Hunger in London. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations, 35*, 417–427. https://doi.org/10.1007/s11266-023-00597-5

Kusimba, S. (2025). Crowdfunding care in Kenya. *Journal of Cultural Economy*, *18*(3), 386–403. https://doi.org/10.1080/17530350.2024.2397375

Ministry of Information, Communications and the Digital Economy. (2025). *Kenya artificial intelligence strategy 2025–2030*. Republic of Kenya. https://ict.go.ke/sites/default/files/2025/03/Kenya%20AI%20Strategy%202025%20-%202030.pdf

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Ndede, V., Miheso, A., Momanyi, D., Kisaka, P., Wanjiku, T., Misiga, Z., & Odhiambo, M. A. (2026). *Data protection manual for non-profit organisations in Kenya: A practical toolkit for managing privacy within your non-profit organisation* (1st ed.). Amnesty International Kenya, DPO 360 Africa Limited, & ICON Data and Learning Labs. https://www.amnestykenya.org/data-protection-manual-for-nonprofit-organisations-in-kenya/

Office of the Data Protection Commissioner. (2024). *Guidance note on data protection impact assessment*. https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-on-Data-Protection-Impact-Assessment-1.pdf

Office of the Data Protection Commissioner. (2025). *Guidance notes for processing children's data*. https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-%E2%80%93-Guidance-Note-for-Processing-Childrens-Data.pdf

Republic of Kenya. (2010). *The Constitution of Kenya, 2010*. National Council for Law Reporting. https://parliament.go.ke/node/161

Republic of Kenya. (2019). *Data Protection Act, No. 24 of 2019*. https://www.odpc.go.ke/data-protection-laws-kenya/

Republic of Kenya. (2021a). *Data Protection (General) Regulations, 2021* (Legal Notice 263 of 2021). https://new.kenyalaw.org/akn/ke/act/ln/2021/263

Republic of Kenya. (2021b). *Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021* (Legal Notice 265 of 2021).

https://new.kenyalaw.org/akn/ke/act/ln/2021/265/eng@2022-12-31

Republic of Kenya. (2022). *Children Act, No. 29 of 2022*. https://new.kenyalaw.org/akn/ke/act/2022/29

United Nations Children's Fund. (n.d.). *Ethical reporting guidelines*. https://www.unicef.org/media/reporting-guidelines

United Nations Children's Fund. (2025). *Guidance on AI and children: Version 3.0*. UNICEF Office of Strategy and Evidence–Innocenti. https://www.unicef.org/innocenti/reports/policy-guidance-ai-children

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. https://www.unesco.org/ethicsai/en/recommendation

United Nations General Assembly. (1989). *Convention on the Rights of the Child*. United Nations.

United Nations General Assembly. (2010). *United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders (the Bangkok Rules)* (A/RES/65/229). United Nations.

United Nations Population Fund, United Nations Children's Fund, & Save the Children. (2025). *Technology-facilitated gender-based violence: Considerations across the life course*. https://www.unfpa.org/resources/technology-facilitated-gender-based-violence-considerations-across-life-course