Privacy and data protection policy and professional and humanitarian code of conduct

Gadim Refugees Empowerment Center (GREC)

Republic of Uganda - Kampala | December 2025

Adoption and hierarchy of instruments

The Board of Directors adopts this Policy as part of the Organization's institutional governance and policy framework. It shall be read with the Constitution, the Board of Directors Rules of Procedure, the Institutional Governance and Administrative Operations Regulations, the Institutional Policy Manual and its Executive Forms Annex. In the event of conflict, applicable Ugandan law prevails, followed by the Constitution, the Regulations, and then this Policy and other policies according to their respective scope.

Nothing in this Policy limits a mandatory reporting duty or lawful cooperation with a competent authority, or authorizes disclosure beyond what is necessary and lawful. The more protective standard shall apply where it is consistent with law and the Organization's obligations.

TABLE OF CONTENTS

PART I

GENERAL PROVISIONS AND GOVERNANCE

Article 1: Purpose

This Policy safeguards the dignity, privacy and safety of persons with whom the Organization interacts; regulates the collection, use and protection of data; establishes professional and humanitarian conduct; prevents abuse of authority, exploitation, discrimination and corruption; and sets clear rules for accountability and incident response.

Article 2: Scope of Application

This Policy applies to members of the General Assembly, Board and committees; the Secretary-General/Chief Executive Officer; staff, volunteers, interns, experts, consultants, contractors, implementing partners, service providers and visitors whenever they act for the Organization, access its data or engage with beneficiaries. It applies in offices, field locations, travel, events, work-related accommodation and digital platforms, and to off-duty conduct materially connected to the Organization, personal safety or public trust.

Article 3: Governing Principles

1. Lawfulness, fairness, transparency and accountability.
2. Humanity, do no harm, non-discrimination, dignity and autonomy.
3. Purpose limitation, data minimization, accuracy and storage limitation.
4. Security, confidentiality, privacy by design and by default.
5. Best interests of the child and a survivor-centered approach.
6. Avoidance of conflicts of interest and non-exploitation of power imbalances or humanitarian need.
7. Due process, proportionality, non-retaliation and continuous learning.

Article 4: Definitions

Term	Approved Meaning
Personal Data	Any information recorded in any form that identifies a person directly or indirectly, including name, contact details, image, case number, location and opinions relating to that person.
Special or Sensitive Personal Data	Data requiring enhanced protection, including health, genetic, biometric, racial or ethnic, religious, sexual and financial data, children's data, protection narratives and records of violations.
Processing	Any automated or non-automated operation performed on data, including collection, recording, organization, analysis, use, disclosure, storage, blocking, erasure and destruction.

Term	Approved Meaning
Data Subject	The natural person to whom personal data relates.
Data Controller / Data Collector / Data Processor	The roles defined by Uganda's Data Protection and Privacy Act according to who determines purposes and means, collects data, or processes it on another party's behalf.
Personal Data Breach	Accidental or deliberate loss, destruction, alteration, disclosure of, or unauthorized access to personal data.
Child	Any person under eighteen years of age.
Beneficiary	Any refugee, asylum seeker, internally displaced person, stateless person, host-community member or other person receiving a service or participating in an activity.
PSEAH	Protection from Sexual Exploitation, Abuse and Harassment.

Article 5: Legal Framework

This Policy shall be applied in accordance with the Constitution of the Republic of Uganda; the Data Protection and Privacy Act, Chapter 97, and the Data Protection and Privacy Regulations, 2021; the Non-Governmental Organizations Act, 2016, as amended; the Employment Act, Chapter 226, as amended through 5 June 2026; the Children Act, Chapter 62, as amended; the Whistleblowers Protection Act, Chapter 34; the Computer Misuse Act, Chapter 96; and any other applicable law or regulatory guidance.

Article 6: Responsibilities and Oversight

1. Board of Directors: approves the Policy, provides oversight and resources, and receives material compliance reports without unnecessary disclosure of victims or whistleblowers' identities.
2. Audit, Risk and Compliance Committee: monitors privacy and conduct risks, material investigations and remediation plans while respecting investigative independence and confidentiality.
3. Secretary-General/Chief Executive Officer: implements the Policy, assigns responsibilities, provides resources and training, and ensures required registrations and regulatory reports.
4. Data Protection Officer: maintains the record of processing activities; manages data-subject requests, impact assessments and the breach register; and coordinates with the Personal Data Protection Office.
5. Safeguarding Officer/PSEAH Focal Point: manages safeguarding referrals, survivor-centered response and child safeguarding.
6. Managers: authorize data collection and access on a need-to-know basis, monitor compliance and report promptly.

7. Every covered person: protects confidentiality, resources and professional boundaries and reports risks and misconduct in good faith.

PART II

PRIVACY AND DATA PROTECTION

Article 7: Record of Processing and Regulatory Registration

The Organization shall maintain an up-to-date record of processing activities identifying data categories, purposes, lawful bases, recipients, storage locations, retention periods and safeguards. It shall register with the Personal Data Protection Office whenever it acts as a data collector, controller or processor, keep its certificate valid, and submit required compliance reports on time.

Article 8: Purpose and Lawful Basis

1. A specific, legitimate and documented purpose shall be identified before collection; data shall not be used for an incompatible new purpose without an appropriate lawful basis and required notice.
2. The lawful basis for each processing activity shall be identified and documented. Consent shall not be relied upon where it is not freely given because of a power imbalance or where assistance is unnecessarily conditional upon it.
3. Consent to receive services shall be separate from optional consent to photography, publication, fundraising or promotional communications.
4. Beneficiary data shall not be sold, exchanged or used for personal, partisan or commercial advantage.

Article 9: Data Minimization and Accuracy

The Organization shall collect only the minimum data necessary, verify accuracy, update data according to risk, and document source and authority. Histories of violations, health, religion, legal status, location or biometric data shall be requested only where necessary, proportionate and authorized.

Article 10: Notice and Transparency

Before collection, or as soon as lawfully practicable, the Organization shall provide a clear notice in an accessible language and format stating its identity and contact details; the data, purpose and lawful basis; whether provision is mandatory or optional; recipients; transfers outside Uganda; retention; rights; and complaint channels. Illiteracy, disability, age, language and humanitarian circumstances shall be accommodated, and oral explanations documented where used.

Article 11: Rights of Data Subjects

1. Receive information about processing and access personal data in accordance with law.

2. Request correction or completion of inaccurate or incomplete data.
3. Object to, or request restriction of, particular processing where permitted by law.
4. Withdraw consent for consent-based processing without retroactively affecting lawful prior processing.
5. Request erasure or destruction where permitted and no legal duty or legitimate basis requires retention.
6. Not be subject to a material decision based solely on automated processing without human review and appropriate safeguards.
7. Complain to the Organization, the Personal Data Protection Office or another competent authority without retaliation.
8. The Data Protection Officer shall register the request, verify identity proportionately, respond within the statutory period, give reasons for any full or partial refusal, and explain the available review or complaint mechanism.

Article 12: Children and Persons at Heightened Risk

1. The best interests of the child shall be a primary consideration. Information shall be age- and capacity-appropriate, with parental or guardian consent or another required lawful basis, and due weight given to the child's views according to maturity.
2. Children's names, images, locations or stories shall not be published where identification may expose them to danger or stigma.
3. Enhanced safeguards apply to survivors of gender-based violence, torture, trafficking and enforced disappearance, and to persons with disabilities, older persons and stateless persons.
4. Assistance shall not be denied because a person refuses photography, publication or optional data collection.

Article 13: Images, Stories, Media and Fundraising

1. Obtain separate, specific, informed and withdrawable consent that is not a condition of assistance.
2. Explain publication channels, audience, approximate duration, and risks of copying and digital dissemination.
3. Use facial obscuring, pseudonyms or generalized locations where disclosure may cause harm.
4. Prohibit degrading, pity-based or staged images, exaggeration, coercion to tell a story, or linking a story to an unexplained financial purpose.
5. Document the material's authorization period, review cycle and withdrawal requests, and remove material where reasonably and lawfully possible.

Article 14: Data Sharing and Disclosure

Data shall be shared only to the extent necessary for a legitimate purpose and on a lawful basis. Aggregated statistics or anonymized data shall be preferred. Requests from public authorities shall be verified for jurisdiction, form, necessity and proportionality; the response shall be documented; and only the minimum required data disclosed.

Article 15: Processors and Partners

Before a partner, supplier or consultant is given access to data, the Organization shall conduct appropriate due diligence and enter into a written agreement covering purpose, instructions, confidentiality, security, sub-processors, assistance with rights and breaches, audit, and return or deletion at the end of the relationship. Reuse or onward transfer requires written authorization and a lawful basis.

Article 16: Transfers outside Uganda and Cloud Services

Data shall not be transferred to, or hosted outside, Uganda until the lawfulness of transfer, level of protection, contractual and technical safeguards, hosting location, potential government access, and recovery and deletion plan have been documented. Additional protection applies to refugee, survivor, child and biometric data.

Article 17: Retention and Disposal

The Secretary-General/Chief Executive Officer shall approve a detailed retention schedule on the recommendation of the Data Protection Officer and record-owning functions. It shall specify owner, purpose, basis, period, disposal method and legal hold. When the purpose ends, data shall be securely erased, destroyed or anonymized; retention shall not be extended merely because of possible future use.

Article 18: Data Protection Impact Assessment

A documented Data Protection Impact Assessment shall precede any high-risk processing, particularly biometric registration, geolocation tracking, large-scale monitoring, database matching, automated processing affecting rights, and databases concerning children, survivors or violations. The activity shall not begin until risks are treated and residual risk is accepted by the competent authority.

PART III

INFORMATION SECURITY, TECHNOLOGY AND COMMUNICATIONS

Article 19: Information Classification and Access

Information shall be classified as Public, Internal, Confidential or Highly Restricted. Access shall use individual accounts, be need-to-know and least-privilege based, be reviewed periodically, and be revoked immediately upon transfer or termination. Account and password sharing is prohibited.

Article 20: Digital and Physical Controls

1. Use strong passwords, multi-factor authentication where available, screen locks, updates and malware protection.
2. Encrypt devices, backups and sensitive media where feasible and proportionate, and test restoration periodically.
3. Do not store sensitive files on personal devices or unapproved media without written authorization and safeguards.
4. Keep paper files in locked cabinets, use a file-loan register and do not leave lists exposed.
5. Verify recipients and attachments before sending, use approved channels and transmit only the minimum necessary.
6. Dispose of records by shredding or irreversible erasure and document destruction of Highly Restricted data.

Article 21: Email, WhatsApp and Social Platforms

1. Do not send case files to personal accounts or public groups, forward messages or take screenshots outside the professional purpose.
2. Do not create lists or groups revealing refugee, health or legal status without necessity and controlled membership and privacy.
3. Review group membership and permissions periodically and remove access immediately when no longer needed.
4. Only authorized persons may publish for the Organization; personal views shall not disclose confidential information or imply an official position.

Article 22: Artificial Intelligence and Automated Tools

1. Personal data, confidential documents or non-anonymized statements shall not be entered into a public AI tool without an impact assessment, written approval and contractual and technical safeguards.
2. Outputs require human verification for accuracy, bias, confidentiality and intellectual-property rights and shall not be treated as final legal or factual authority.
3. No solely automated decision shall accept or reject a beneficiary or employee, refer a case or determine eligibility without human review and a right to challenge.

4. Approved tools, purposes, data, decision logs and risk reviews shall be documented.

Article 23: Acceptable Use of Organizational Resources

Devices, accounts, connectivity and software shall be used for lawful and professional purposes. Unauthorized access, circumvention of controls, installation of unapproved software, hosting illegal or abusive content, and personal, partisan or commercial use are prohibited. Technical monitoring shall be lawful, proportionate and transparent to the extent permitted by law.

Article 24: Personal Data Breach Management

Every person shall immediately report loss, misdirected transmission, unauthorized access or suspected breach without waiting for complete information. The Data Protection Officer shall lead containment and preservation of evidence, assess the data type, number of persons, identifiability, likelihood of harm and vulnerable groups, and document the notification decision. The Organization shall immediately notify the Personal Data Protection Office of a breach likely to place personal data at risk and shall notify affected data subjects where required by law or necessary for protection, explaining protective steps without undue delay.

PART IV

PROFESSIONAL AND HUMANITARIAN CODE OF CONDUCT

Article 25: Duties of Conduct

1. Treat everyone with dignity, respect, fairness and due regard to culture, language, religion, disability, age, sex and legal status.
2. Perform work honestly, competently and carefully, maintaining neutrality, independence and do-no-harm.
3. Provide accurate information about services, resources and results and do not make promises beyond authority.
4. Protect organizational assets, time and reputation and do not use them for personal or partisan benefit.
5. Maintain professional boundaries and do not enter exploitative or inappropriate dependency relationships with beneficiaries.
6. Promptly disclose conflicts, gifts and relationships that may influence or appear to influence a decision.
7. Follow safety and security instructions and report risks and incidents.

Article 26: Non-Discrimination, Harassment and Bullying

The Organization prohibits discrimination, harassment, bullying, hate speech, humiliation and retaliation in any form. Reasonable accommodation shall be provided for persons with disabilities

where required and equal opportunity and due process applied in accordance with Ugandan law and approved policies.

Article 27: Protection from Sexual Exploitation, Abuse and Harassment

1. Requesting or accepting sexual activity or benefit in exchange for money, employment, assistance, protection, service or preferential treatment is prohibited.
2. Any sexual activity with a person under eighteen is prohibited regardless of purported consent or mistaken age.
3. Exploitation of power, need or confidentiality, and relationships that breach professional boundaries or create a material conflict, are prohibited.
4. Unqualified persons shall not investigate survivors. Response must be confidential, survivor-centered, safe and child-appropriate, with informed-consent referrals unless law requires otherwise.

Article 28: Safeguarding Children and Adults at Risk

1. Violence, neglect, exploitation, and physical, psychological, economic or digital abuse are prohibited.
2. Unnecessary one-to-one meetings with a child in a closed place, and secret personal contact outside approved professional channels, are prohibited.
3. A child shall not be employed or assigned hazardous, degrading or age-inappropriate activity.
4. Safeguarding concerns shall be reported immediately through the approved channel; immediate safety takes priority over administrative considerations.

Article 29: Conflicts of Interest and Gifts

A person shall disclose in writing any actual, potential or perceived conflict immediately upon becoming aware of it and shall abstain from related discussion, assessment, recommendation, voting or contracting until a documented decision is issued. Cash gifts, commissions, bribes and any gift or hospitality that influences or appears to influence a decision are prohibited. Permitted gifts shall be recorded under the applicable policy and Board-approved threshold.

Article 30: Gross Prohibitions

1. Fraud, embezzlement, bribery, extortion, forgery or manipulation of beneficiary lists, procurement or reports.
2. Retaliation against a whistleblower, complainant, witness or person refusing an unlawful instruction.
3. Disclosure or use of data or secrets for threats, benefit, propaganda or political targeting.
4. Weapons, violence or threats in organizational activities except under lawful and approved security arrangements.
5. Working under the influence of alcohol or drugs where persons or work is endangered.

6. Making a statement, commitment or political position for the Organization without authorization.
7. Obstructing an investigation, destroying evidence, influencing witnesses or deliberately providing false information.

PART V

REPORTING, RESPONSE AND ACCOUNTABILITY

Article 31: Reporting and Complaint Channels

The Organization shall provide multiple safe, accessible and publicized channels, including a written channel, dedicated telephone or WhatsApp line, and complaint box and in-person interview. An alternative channel outside the management line shall be available where a report concerns a senior official or receiving officer. Anonymous reports shall be accepted to the extent they can be assessed. Internal reporting is not a prerequisite to contacting the police, Personal Data Protection Office, National Bureau for NGOs or another competent authority.

Article 32: Non-Retaliation and Confidentiality

Dismissal, intimidation, benefit reduction, defamation, threats, isolation or any adverse treatment because of a good-faith report, exercise of a right or participation in an investigation is prohibited. Information shall be restricted to need-to-know. An unsubstantiated report is not malicious unless intentional lie is established. Immediate and proportionate protective measures shall be taken for the reporter, complainant, survivor and witnesses.

Article 33: Triage, Referral and Initial Response

Situation	Required Initial Action
Risk to life or safety	Secure the person and seek appropriate emergency or protection services without creating additional risk.
PSEAH allegation or gender-based violence	Apply strict confidentiality, survivor-centered response, consent-based specialist referral and no unqualified questioning.
Child safeguarding concern	Apply the best interests principle, prevent unnecessary contact, and refer immediately to the safeguarding focal point and competent authorities where required.
Personal data breach	Contain the breach, preserve evidence, notify the Data Protection Officer immediately and assess regulatory and individual notification.
Fraud or corruption	Preserve records, restrict access, refer independently and prevent interference with records or witnesses.

Situation	Required Initial Action
Complaint against receiving officer	Use the alternative channel and exclude the subject from receipt, investigation and decision.

Article 34: Investigation and Due Process

Investigations shall be independent, impartial, competent and confidential, with clear jurisdiction, plan and evidence preservation. The subject shall be informed of the allegation without endangering a victim or evidence and given a fair opportunity to respond. Wherever possible, receipt, investigation, decision and appeal shall be separated. Internal settlement shall not prevent exercise of a legal right or reporting to a competent authority.

Article 35: Measures, Sanctions and Referral

Measures shall be proportionate to misconduct, harm, risk, record and cooperation and may include guidance, training, warning, access restriction, recovery, suspension, termination of membership, service, contract or partnership, and referral to a regulator or law-enforcement body. Interim measures protect persons and evidence and do not prejudge guilt. Review and appeal rights shall be respected under approved instruments and law.

PART VI

IMPLEMENTATION, REVIEW AND ENTRY INTO FORCE

Article 36: Training and Acknowledgement

Every covered person shall receive induction on this Policy before or upon commencement and sign an acknowledgement. Training shall occur at least annually on privacy, information security, the Code of Conduct, PSEAH, child safeguarding and conflicts of interest, with specialist training for high-risk roles.

Article 37: Records, Monitoring and Reporting

1. Record of processing activities, data-subject requests and consents.
2. Registers of access rights, transfers, processors, partners and impact assessments.
3. Register of breaches, complaints, investigations and sanctions, with investigation files separated from general operational records.
4. Indicators for training, response, closure, recurrence and remediation plans.
5. Periodic reporting to the Secretary-General/CEO and Audit, Risk and Compliance Committee, and an annual report to the Board without unnecessary identities.

Article 38: Review and Exceptions

The Policy shall be reviewed annually or upon a change in law or regulatory guidance, material programmer or technology change, material incident, or audit finding requiring amendment. No exception may be granted to prohibitions on exploitation, abuse, bribery or retaliation, or to a legal duty. Any other operational exception must be written, reasoned, time-limited, supported by compensating controls and approved by the competent authority after advice from the Data Protection Officer or compliance function, as applicable.

Article 39: Interpretation and Entry into Force

The Board shall interpret this Policy consistently with law, the Constitution and Regulations and may obtain independent legal advice. The Policy enters into force upon adoption by Board resolution and supersedes any earlier privacy policy or code of conduct within its subject matter.

ANNEX A: SIMPLIFIED PRIVACY NOTICE FOR BENEFICIARIES

GREC respects your privacy and dignity. We collect only the information needed to provide services, operate programs safely and meet legal obligations. We will explain why information is requested, whether it is necessary, who may access it, how long it is retained and how it is protected.

1. Refusing photography or publication will not prevent you from receiving assistance.
2. You may request access to or correction of your data, or ask how it is used, in accordance with law.
3. Do not pay money or give a gift or personal benefit to any worker in exchange for an organizational service.
4. You may complain or report through the publicized official channels without fear of retaliation.
5. If your privacy complaint is not resolved, you may contact Uganda's Personal Data Protection Office.

An organizational worker will explain this notice orally or in an appropriate language or format where needed.

ANNEX B: ACKNOWLEDGEMENT AND COMMITMENT FORM

I acknowledge that I have received, read and understood GREC's Privacy and Data Protection Policy and Professional and Humanitarian Code of Conduct. I undertake to comply with it, protect information and report misconduct during and after my service. I understand that a breach may result in disciplinary, contractual, regulatory or legal action.

Field	To Be Completed
Full Name	
Capacity / Position	
Department / Project	
Official Telephone / Email	
Signature	
Date	
Name and Signature of Organizational Recipient	

ANNEX C: INDICATIVE RECORDS-RETENTION SCHEDULE

A detailed schedule shall be adopted separately after reviewing the legal and contractual requirements for each category. The following controls are indicative and shall not create retention longer than necessary:

Record Category	Retention and Review Rule
Beneficiary and Case Files	Review upon case closure; retain only for the necessary or legally or contractually required period, then erase or anonymize.
Media Images and Stories	Review consent and publication cycle periodically; remove when purpose ends or consent is withdrawn where legally and practically possible.
Employment and Financial Records	Retain under the Employment Act as amended in 2026, tax, audit and contract requirements, and the approved records schedule.
Unsuccessful Job Applications	Retain for a limited and disclosed period, then securely erase unless a lawful basis or separate specific consent supports further retention.
Complaints and Investigations	Restrict access and retain proportionately to justice, accountability, risk and legal obligations.
Consent, Rights-Request and Breach Records	Retain long enough to evidence compliance and resolve disputes under law and the records schedule.

ANNEX D: INITIAL PERSONAL DATA BREACH RESPONSE CARD

1. Stop the leak or restrict access without destroying evidence.
2. Notify the Data Protection Officer immediately; do not wait for complete details.
3. Record the time, systems, data, persons, recipients and actions taken.
4. Assess likely harm, particularly to children, refugees, survivors and persons at heightened risk.
5. Decide and document immediate notification to the Personal Data Protection Office and individual notification in accordance with law.
6. Address the root cause, support affected persons, and review controls and training.

LEGAL AND REGULATORY REFERENCES

1. Constitution of the Republic of Uganda, particularly the rights to privacy, equality and fair procedure.
2. Data Protection and Privacy Act, Chapter 97 (Act No. 9 of 2019, in the Revised Laws through 31 December 2023).
3. Data Protection and Privacy Regulations, 2021, Statutory Instrument No. 21 of 2021.
4. Non-Governmental Organizations Act, 2016, as amended, including the 2024 amendment effective 30 September 2024, and the NGO Regulations, 2017.
5. Employment Act, Chapter 226, as amended by the Employment (Amendment) Act, 2026, effective 5 June 2026.

6. Children Act, Chapter 62, as amended through 16 August 2024.
7. Whistleblowers Protection Act, Chapter 34, and Computer Misuse Act, Chapter 96.
8. Guidance, forms and compliance tools issued by Uganda's Personal Data Protection Office.

ADOPTION AND APPROVAL

1. Adopted by the General Assembly at its meeting held on 31 December 2025.
2. The General Assembly authorizes the Board Chairperson and Legal Adviser to sign on behalf of all members and the Organization's official seal shall be affixed.

Signature of the Board Chairperson: **Signature of the Legal Adviser:**