Justice Revived Foundation (JRF)

Data Protection & Privacy Policy
Version 1.0 │ Approved: _20_ / _01_ / 2025 │ Next Review: January 2027
This policy provides governance and internal controls for JRF. It is not legal advice.

Table of Contents

1) Purpose, Scope & Legal Basis

Purpose. To ensure that personal data handled by JRF is processed lawfully, fairly, securely and transparently; to protect the rights of data subjects; and to embed accountable privacy practices across programmes, HR, finance, MEL and partnerships.

Scope. Applies to all personal data processed by or on behalf of JRF (employees, applicants, volunteers, beneficiaries, vendors, partners, donors, website users), in any format (paper, audio, images, digital, cloud) and any location.

Legal Basis. JRF complies with Ghana's Data Protection Act, 2012 (Act 843) and guidance from the Data Protection Commission (DPC). Where donor or international standards are stricter, JRF applies the stricter standard.

Registration. JRF will register with the Data Protection Commission as required by Act 843 and maintain current registration details.

2) Definitions

- **Personal data:** Information relating to an identifiable natural person.

- **Special category/sensitive data:** Data relating to health, biometrics, sexual life, child data, and other data treated as sensitive by JRF.
- **Processing:** Any operation on personal data (collect, store, use, disclose, destroy).
- **Data Controller:** The entity determining the purpose/means of processing (JRF).
- **Data Processor:** A third party processing data on JRF's behalf.
- **DPO:** Data Protection Officer (JRF role for compliance coordination).
- **DSAR:** Data Subject Access Request.
- **Anonymisation / Pseudonymisation:** Irreversible removal / reversible separation of identifiers.

3) Principles of Processing

JRF adopts privacy principles consistent with Act 843 and international good practice:

1. **Lawfulness, fairness & transparency**
2. **Purpose limitation** (specified, explicit, legitimate purposes)
3. **Data minimisation** (adequate, relevant, limited)
4. **Accuracy** (kept up-to-date)
5. **Storage limitation** (no longer than necessary)
6. **Integrity & confidentiality** (security by design)
7. **Accountability** (evidence of compliance; audit trails)

4) Roles, Governance & RACI

4.1 Roles & Responsibilities

- **Board of Directors:** Approves policy; receives annual privacy report and significant incident updates.
- **Executive Director (ED):** Accountable for compliance; ensures resources and risk management.
- **Data Protection Officer (DPO):** Policy custodian; registration with DPC; oversees DSARs, DPIAs, breach response; training; vendor privacy due diligence; liaison with the DPC.
- **Data Owners (Dept Heads):** Define purposes; approve retention; ensure local controls.
- **Data Stewards (Ops/MEL/HR/IT):** Maintain records of processing; implement controls; ensure data quality.
- **IT & Security Lead:** Implements technical safeguards, access control, backups, and incident detection.
- **All Staff & Partners:** Comply with this policy; complete training; report incidents immediately.

4.2 RACI (selected processes)

Process	Board	ED	DPO	Data Owner	IT Sec	Staff
Policy approval	A/R	C	C	I	I	I
DPC registration	I	C	A/R	I	I	I
DSAR handling	I	C	A/R	R	C	C

Process	Board	ED	DPO	Data Owner	IT Sec	Staff
DPIA reviews	I	C	A/R	R	C	I
Breach response	I	A	R	R	R	C
Vendor assessments	I	C	A/R	R	C	I

A=Accountable, R=Responsible, C=Consulted, I=Informed

5) Lawful Bases for Processing

JRF documents a lawful basis for each processing activity (Annex A: Data Inventory/RoPA template). Common bases include:

- **Consent** (e.g., use of images on website; some research activities).
- **Contract** (e.g., employment, vendor agreements, stipends).
- **Legal obligation** (e.g., tax, social security, safeguarding reports).
- **Vital interests** (e.g., emergency medical disclosures).
- **Legitimate interests** (balanced against rights; e.g., M&E improvements, limited security CCTV).

Where consent is used, it must be freely given, specific, informed and unambiguous, with an easy withdrawal process.

6) Children's Data & Vulnerable Persons

- **Child**: under 18 years (Children's Act, 1998).
- Processing children's data requires enhanced safeguards and, where appropriate, parental/guardian consent plus child assent (Annex G).
- For safeguarding and PSEA cases, confidentiality is paramount; information is shared strictly on a **need-to-know** basis and in line with legal/reporting obligations and JRF Safeguarding/PSEA Policies.

7) Data Collection, Notices & Consent

- **Privacy Notices:** JRF provides clear, accessible notices tailored to the audience (beneficiaries, staff, website users, see Annex F).
- **Minimum data:** Only collect what is necessary for a defined purpose.
- **Consent management:** Record who consented, when, for what, and how to withdraw; do not bundle consent with unrelated services.
- **Audio/visual media:** Use signed consent forms; anonymise where feasible; avoid publishing content that risks harm.

8) Data Minimisation, Quality & Retention

- **Data quality:** Owners ensure timely updates and corrections.
- **Retention:** Keep only as long as needed for the stated purpose, legal limitation periods, or donor requirements; then securely delete or anonymise.
- **Retention Schedule:** See Annex D (e.g., HR records = employment + 7 years; PSEA/safeguarding case files = 10 years or until child turns 25, whichever is longer; finance & tax = 10 years).

9) Security Measures (Organisational, Physical, Technical)

Organisational

- Role-based access control; least privilege; NDA/confidentiality in contracts.
- Clear-desk and secure printing; visitor controls; locked cabinets for paper files.
- Security in procurement: privacy in RFPs; vendor due diligence (Annex E).

Physical

- Controlled office access; locked file rooms; CCTV where justified (see §14).
- Secure storage for evidence (safeguarding/PSEA).

Technical

- Device encryption; MFA for email/cloud; strong passwords with expiry; automatic screen locks.
- Network security: firewalls, endpoint protection, patching policy, restricted admin rights.
- Backups and disaster recovery tested periodically.
- Data in transit via TLS; sensitive data at rest with AES-256 encryption where feasible.
- Audit logs for access to high-risk systems (safeguarding, HR, finance).

10) Data Sharing, Vendors & International Transfers

- **Third parties:** Only engage processors with appropriate safeguards; sign Data Processing Agreements (DPAs) using JRF template (Annex E).
- **Purpose limitation:** No secondary use by vendors without JRF's written instruction.
- **Cross-border transfers:** Assess legal mechanisms and risks (e.g., contractual safeguards). Where required by Act 843 or DPC, obtain authorisations/assurances before transfer. Use the Cross-Border Assessment section in Annex A and related guidance.

11) Data Subject Rights & Requests (DSARs)

Individuals may exercise rights under Act 843, which include (as applicable): access, rectification/correction, objection, erasure (subject to legal limits), restriction, and objection to direct marketing.

JRF DSAR process

- **Submit:** Using the DSAR Form (Annex A/F) or via email/letter.
- **Acknowledge: Within 5 working days** with case reference.
- **Respond: Within 30 calendar days** (extend once with justification where permitted).
- **Verify identity** before disclosure; redact third-party data where necessary.
- Keep an **audit trail** of all DSARs.

12) DPIAs (Data Protection Impact Assessments)

Required for **high-risk** processing (e.g., large-scale children's data, sensitive health data, tracking, biometric systems, geolocation, profiling).

Process (Annex C DPIA template):

1. Describe processing & purpose → 2) Assess necessity/proportionality → 3) Identify risks to rights/freedoms → 4) Define mitigations → 5) DPO review & sign-off → 6) Implement controls before go-live.

13) Data Breach Management & Notification

A **personal data breach** is any security incident leading to accidental/unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

JRF Breach SOP (Annex B):

- **Report immediately** to DPO/IT (any staff member).
- **Triage** within **24 hours** (scope, data types, affected people, ongoing risk).
- **Contain & remediate** (isolate systems, reset credentials, notify vendors if implicated).
- **Notify**: JRF commits to notify the Data Protection Commission and affected individuals without undue delay where required or appropriate; JRF's **internal target** is to complete assessment within **72 hours** to decide on notification.
- **Document** all breaches (even minor) in the Breach Register; lessons learned feed into training and controls.

14) Marketing, Cookies, CCTV & Research Data

- **Direct marketing:** Use clear opt-in/opt-out; honour objections; do not share lists without basis.
- **Cookies/Website:** Provide a Cookie & Privacy Notice (Annex F) detailing purposes, types, and choices.
- **CCTV (if used):** Signage, narrow purpose (safety/security), limited retention, controlled access; no audio unless justified.
- **Research & M&E:** Prefer anonymised or pseudonymised datasets; ethics checks where appropriate; ensure consent or another lawful basis; avoid re-identification.

15) Training, Awareness & Disciplinary Measures

- **Training:** Mandatory induction and annual refresher for all staff; role-specific training for HR, MEL, IT, and investigators.
- **Contractual clauses:** Confidentiality and data protection obligations in all staff and vendor contracts.
- **Discipline:** Breaches of this policy may lead to disciplinary action up to dismissal and possible legal action; vendor breaches may trigger contract termination and debarment.

16) Monitoring, Audits, KPIs & Reporting

- **KPIs (quarterly):**
  - % staff completing privacy training
  - and outcome of DSARs; average response days
  - of DPIAs completed; mitigations implemented

    - of incidents/breaches; time to containment
    - Vendor DPA coverage (% of in-scope vendors)
- **Audits:** Annual privacy audit by DPO; targeted spot checks for high-risk areas; report to ED/Board.
- **Records of Processing:** Maintained by Data Owners using Annex A (RoPA).

17) Policy Review & Change Control

- **Scheduled review** every 12-24 months (next by January 2027) or earlier upon legal/donor changes, new technologies, or incidents.
- **Change process:** DPO drafts → consultation → ED review → Board approval → version control and staff briefing within 10 working days.

18) Annexes (Templates & Tools)

A. Data Inventory & Record of Processing Activities (RoPA) Template
B. Data Breach Report Form & Incident SOP
C. DPIA Template & Guidance
D. Data Retention Schedule (by dataset)
E. Third-Party Data Processing Agreement (DPA) Template
F. Privacy Notice Templates (Beneficiaries, Staff, Website/Cookies)
G. Consent Forms (Adults; Parental + Child Assent)

Prepared by: Data Protection Officer
Approved by: Executive Director & Board Chair
Date: __ / __ / 2025