ACCET

AFRICA CENTRE FOR CRITICAL MINERALS & ENERGY TRANSITION

Guiding Policy

DATA PROTECTION & PRIVACY POLICY

Approved by the Governing Council: March 2026

www.accetafrica.org

Data Protection & Privacy Policy

1. Purpose

This policy sets out ACCET's commitment to protecting the privacy and personal data of all individuals whose data we process, in accordance with the **Data Protection Act, 2012 (Act 843)** of Ghana, the **Electronic Transactions Act, 2008 (Act 772)**, and other relevant legislation.

2. Scope

This **Data Protection & Privacy Policy** applies comprehensively to all activities of the **Africa Centre for Critical Minerals & Energy Transition (ACCET)** involving the collection, processing, storage, sharing, and disposal of personal data.

Specifically, it covers:

1. Data Subjects

- **Employees, fellows, interns, and consultants** – including HR records, performance data, payroll, and benefits information.
- **Job applicants and candidates** – including CVs, references, interview notes, and background checks.
- **Partners and stakeholders** – including representatives of governments, private sector, academia, civil society, and donors whose contact details and correspondence are maintained.
- **Beneficiaries and participants** – individuals and communities engaged in ACCET's programs, surveys, workshops, research, and events.
- **Vendors and suppliers** – business contact details, contracts, and compliance documentation.
- **Website visitors and digital users** – data collected via cookies, analytics tools, newsletters, and contact forms.

---

2. Data Types Covered

- **Basic personal data:** Names, gender, addresses, phone numbers, email addresses.
- **Identification data:** Passport numbers, national IDs, staff numbers.
- **Employment data:** Contracts, payroll, appraisal records, leave records, disciplinary actions.
- **Financial data:** Bank account details, payment histories, grant disbursements.
- **Special personal data (sensitive data):** Health information, ethnicity, religious affiliation, biometric data, political affiliation, where relevant for lawful or programmatic reasons.
- **Digital data:** IP addresses, cookies, geolocation data, photos, audio/video recordings from events.
- **Research data:** Survey responses, interview recordings, focus group discussions, anonymized case studies.

---

3. Activities Covered

- **Recruitment & HR management** – collection and processing of staff/fellow data from application to exit.
- **Program implementation & research** – surveys, interviews, monitoring & evaluation, capacity-building initiatives.
- **Partnerships & stakeholder engagement** – managing contacts and communications with governments, donors, academia, industry, and civil society.
- **Procurement & contracting** – vendor vetting, supplier data, and compliance checks.
- **Financial operations** – payroll, donor reporting, grant management, reimbursements.
- **ICT & digital platforms** – website operations, mailing lists, social media engagement, and virtual conferencing.
- **Advocacy & communications** – photography, video, and audio recording of events and publications (with consent).
- **Data sharing & cross-border transfers** – sharing with donors, research partners, or service providers under lawful contracts and safeguards.

---

4. Systems & Locations

This policy applies to:

- **All ACCET offices** in Ghana and any regional/international branches.
- **All IT systems and databases** owned, leased, or hosted by ACCET.
- **Cloud storage platforms** (e.g., Microsoft 365, Google Workspace, donor-mandated systems).
- **Physical records** (e.g., paper files, signed contracts) maintained at ACCET offices.
- **Third-party hosted systems** where ACCET data is stored or processed.

---

5. Third Parties

This policy extends to **external parties** that ACCET contracts or partners with to process personal data on its behalf, including:

- Consultants, auditors, and IT providers.
- Research partners and subcontractors.
- Donors who require data access for project monitoring.
- Vendors and suppliers accessing or handling ACCET data.

All third parties must sign **Data Processing Agreements** and comply with this policy.

---

3. Key Definitions

- **Personal Data:** Information that can identify an individual (e.g., name, contact details, ID number).
- **Special Personal Data:** Sensitive categories under Act 843 such as health, race, ethnic origin, political opinions, religion, sexual life, and criminal records
- **Data Subject:** An individual whose data is being processed.
- **Data Controller:** ACCET, which determines why and how personal data is processed.
- **Data Processor:** Third parties engaged by ACCET to process data.

---

4. Data Protection Principles

ACCET shall process all personal data in line with these principles:

1. **Lawfulness & Fairness:** Data shall be processed lawfully and fairly.
2. **Purpose Limitation:** Data collected for specified purposes shall not be used for incompatible purposes.
3. **Data Minimization:** Only data necessary for the stated purpose shall be collected.
4. **Accuracy:** Data shall be kept accurate and up to date.
5. **Storage Limitation:** Data shall not be retained longer than necessary.
6. **Security Safeguards:** Data shall be protected against loss, damage, or unauthorized access.
7. **Accountability:** ACCET shall ensure compliance and demonstrate responsibility.

---

5. Lawful Basis for Processing

Personal data shall be processed on one or more of the following grounds:

- Consent of the data subject.
- Fulfilment of a contract.
- Compliance with a legal obligation.
- Protection of vital interests of the data subject.
- Legitimate interests of ACCET balanced against rights of the data subject.

---

6. Data Subject Rights

ACCET respects and upholds the rights of data subjects, including:

- Right to be informed of data processing.
- Right to access personal data.
- Right to correct or rectify inaccurate data.
- Right to prevent processing likely to cause harm.
- Right to object to direct marketing.
- Right to request deletion (subject to lawful retention requirements).

Requests shall be addressed within **30 days** of receipt.

---

7. Special Categories of Data

Processing of special personal data (e.g., health, ethnicity, religion, children's data) shall be subject to explicit consent of the data subject, or permitted only under the lawful exceptions in Act 843.

---

8. Data Security Measures

ACCET is committed to safeguarding all personal data against unauthorized access, alteration, disclosure, or destruction. Data security will be ensured through a layered approach that combines **technical, organizational, and physical controls**:

A. Technical Measures

- **Encryption:** All sensitive digital data (financial, HR, research) will be encrypted both in transit (SSL/TLS for emails/websites) and at rest (on servers, laptops, and cloud storage).
- **Access Controls:** Role-based access with passwords, two-factor authentication (2FA), and automatic log-out.
- **Secure IT Infrastructure:** Use of firewalls, anti-malware software, and intrusion detection systems.
- **Data Backups:** Regular, encrypted backups stored offsite or in secure cloud servers; tested periodically for restoration.
- **Audit Logs:** IT systems will maintain logs of access and changes to sensitive data, reviewed quarterly.

B. Organizational Measures

- **Confidentiality Agreements:** All staff, interns, fellows, and contractors must sign data confidentiality clauses in contracts.
- **Data Classification:** Personal data categorized by sensitivity (public, restricted, confidential, highly confidential).
- **Training:** Mandatory annual training on data protection, phishing risks, and cyber hygiene for all staff.
- **Data Minimization:** Collect only data necessary for defined purposes; anonymize where possible (e.g., research datasets).
- **Incident Response:** A documented Data Breach Response Plan with reporting, containment, and corrective measures.

C. Physical Measures

- Secure offices with access control (ID cards, visitor logs).
- Locked filing cabinets for hard-copy records.
- Shredding of obsolete paper documents.
- Secure storage of backup devices and restricted server rooms.

---

9. Cross-Border Data Transfers

ACCET recognizes that certain operations, research collaborations, and donor reporting require the transfer of personal data across national borders.

A. Legal Compliance

- Data transfers shall comply with **Section 40 of Ghana's Data Protection Act (Act 843)**, which restricts transfers to jurisdictions that ensure an adequate level of protection.
- Where the recipient country lacks adequate laws, transfers will only proceed under:
    - Explicit consent of the data subject.
    - A binding contract with the recipient guaranteeing equivalent protection.
    - A necessity for performance of a contract or legal obligation.

B. Safeguards for Transfers

- **Data Transfer Agreements (DTAs):** All international transfers will be governed by contracts that specify purpose, security measures, retention, and data subject rights.
- **Donor/Partner Transfers:** Data shared with donors or research partners abroad will be anonymized where possible, or shared under strict non-disclosure clauses.
- **Cloud Providers:** ACCET will use only reputable providers (Microsoft, Google, AWS, etc.) that comply with international standards such as GDPR and ISO 27001.
- **Audit Rights:** ACCET reserves the right to review compliance of foreign processors or partners.

C. Transparency to Data Subjects

- Individuals will be informed at the point of collection if their data may be transferred abroad, including the purpose and recipient country.

---

10. Cookies & Website Data

ACCET's website and online platforms are important tools for communication, research dissemination, and stakeholder engagement. We are committed to handling all digital user data responsibly.

A. Cookies and Tracking Technologies

- **Types of Cookies Used:**
  - *Essential cookies* – required for basic website functionality (e.g., log-in, secure browsing).
  - *Performance cookies* – track website usage statistics (e.g., pages visited, session duration) to improve user experience.
  - *Functionality cookies* – remember user preferences (e.g., language, region).
  - *Analytics & third-party cookies* – may be used through Google Analytics or similar tools to assess reach and performance.
- **User Consent:**
  - Visitors will be notified via a cookie banner/pop-up upon their first visit.
  - Users can accept, reject, or customize cookie preferences.
  - Consent can be withdrawn at any time by adjusting browser or cookie settings.

B. Website Data Collected

- IP addresses, browser type/version, operating system, referral pages, and session duration.
- Information voluntarily provided via **contact forms, newsletter sign-ups, event registrations, or surveys**.
- Social media interactions embedded on the website (e.g., LinkedIn or Twitter plug-ins).

C. Use of Website Data

- To improve website functionality, content relevance, and accessibility.
- To monitor security and detect fraudulent or malicious activity.
- To manage subscriptions to newsletters and event updates.

D. Storage and Sharing

- Website analytics data will be anonymized where possible.
- Raw logs will be stored securely and deleted within **12 months** unless required for legal or security investigations.
- Data will not be sold or shared with third parties except with trusted service providers under written agreements.

---

11. Data Breach Notification

- Any suspected or actual personal data breach must be reported immediately to the **Data Protection Supervisor**.
- The **Data Protection Commission** shall be notified **as soon as possible** after discovery of a serious breach, as required under Act 843【web.run†source】.
- Affected individuals will also be informed where there is a risk of harm.

---

12. Roles & Responsibilities

A. Governing Council

- Provides overall oversight on compliance with legal and donor requirements.
- Approves key data protection policies and reviews annual data protection reports.

B. Executive Director (ED)

- Holds ultimate accountability for data protection and privacy compliance.
- Ensures resources are allocated for data protection (staff, training, IT security).
- Reports breaches or serious risks to the Governing Council.

C. Data Protection Officer (DPO)

- Acts as the focal point for all data protection matters.
- Monitors compliance with Ghana's Data Protection Act and donor requirements.
- Maintains a **data processing register** of all personal data handled by ACCET.
- Handles Data Subject Access Requests (DSARs).
- Provides guidance on data protection impact assessments (DPIAs).
- Reports notifiable breaches to the **Data Protection Commission (DPC) of Ghana** within statutory timelines.

D. Heads of Departments & Project Leads

- Ensure compliance within their teams (HR, Finance, Research, Programs).

- Identify and classify personal data processed in their operations.
- Train and supervise staff handling sensitive data.

E. Employees, Interns & Fellows

- Must follow this policy and handle data securely in daily tasks.
- Required to immediately report suspected breaches, loss of devices, or unauthorized disclosures.
- Prohibited from copying or disclosing personal data without authorization.

F. IT & Systems Administrators

- Maintain secure IT infrastructure and apply patches/updates regularly.
- Monitor access logs and report suspicious activity.
- Support encryption, access control, and secure storage.

G. Third-Party Processors (Vendors, Contractors, Partners)

- Must sign **Data Processing Agreements** with ACCET.
- Required to apply equivalent security measures to protect ACCET's data.
- Must notify ACCET within 24 hours of discovering a breach.

---

13. Policy Review

This policy shall be reviewed every **two years** or earlier if required by law or organizational changes.

---

14. Effective Date

This policy is effective from **[insert date]** and applies to all operations of ACCET in Ghana and abroad.

ACCET

DT Plaza, Boundary Road West Wing -
2nd Floor East Legon, Accra

www.accetafrica.org | **info.accetafrica.org**

+233 303 965259