# **Data Protection and Privacy Policy**

# **Women's Shelter Services, Kenya**

### 1. Policy Objectives

* Protect survivor personal information
* Ensure data confidentiality
* Comply with Kenyan Data Protection Act
* Safeguard survivor privacy rights

### 2. Legal Compliance

2.1 Regulatory Framework

* Data Protection Act (2019)
* Constitution of Kenya
* International human rights standards
* Victim protection guidelines

2.2 Key Legal Principles

* Consent-based data processing
* Minimal data collection
* Purpose limitation
* Data subject rights
* Security safeguards

### 3. Data Collection Protocols

3.1 Permitted Data Collection

* Basic identification information
* Case management details
* Safety assessment data
* Service intervention records

3.2 Prohibited Data Collection

* Unnecessary personal details
* Speculative or discriminatory information
* Unrelated third-party data

### 4. Data Management

4.1 Collection Procedures

* Informed consent
* Voluntary information sharing
* Clear purpose explanation
* Right to refuse

4.2 Storage Mechanisms

* Encrypted digital systems
* Secure physical filing
* Access-controlled environments
* Regular data audits

### 5. Survivor Rights

5.1 Information Rights

* Access personal data
* Request data modification
* Demand data deletion
* Challenge information accuracy

5.2 Consent Management

* Revocable consent
* Age-appropriate mechanisms
* Transparent withdrawal process

### 6. Data Security Measures

6.1 Technical Protections

* End-to-end encryption
* Secure cloud storage
* Multi-factor authentication
* Regular security updates

6.2 Physical Security

* Locked file systems
* Restricted physical access
* Secure document destruction
* Staff background checks

### 7. Data Sharing Guidelines

7.1 Permitted Sharing

* Legal mandatory reporting
* Imminent safety risks
* Interdepartmental case management
* With explicit survivor consent

7.2 Prohibited Sharing

* Unauthorized third-party access
* Media or public disclosure
* Personal networking
* Discriminatory information exchange

### 8. Staff Responsibilities

8.1 Training Requirements

* Annual privacy training
* Confidentiality agreements
* Ethical data handling
* Regular compliance updates

8.2 Accountability

* Personal data protection commitment
* Immediate breach reporting
* Professional consequences for violations

### 9. Breach Response Protocol

9.1 Notification Procedures

* Immediate survivor communication
* Comprehensive investigation
* Remediation strategies
* Legal compliance

9.2 Mitigation Steps

* Data recovery
* Security system review
* Potential legal actions
* Preventive future measures

### 10. Policy Review

* Annual comprehensive review
* Stakeholder input
* Legal landscape monitoring
* Continuous improvement

Effective Date: [Current Date] Next Review: [One Year from Effective Date]