INITIATIVE FOR LEGAL AID

(ILA)

DATA PROTECTION AND PRIVACY POLICY

Version: 1.0

Effective Date: _____

Approved by: Board of Directors

Policy Owner: Executive Director

Responsible Department: Administration and ICT

Review Date: Every two (2) years or as required.

INITIATIVE FOR LEGAL AID (ILA)

DATA PROTECTION AND PRIVACY POLICY

Policy Number: ILA/POL/DPP/001/2026

Version: 1.0

AMENDMENT RECORD

This Policy shall remain a living document. Amendments may be proposed by Management, the ICT Unit, the Legal Unit, the Executive Director, or the Board of Directors. No amendment shall become effective unless approved by the Board of Directors.

Minor administrative amendments that do not alter the substance of this Policy, including updates to annexes, forms, contact details, or statutory references, may be approved by the Executive Director and reported to the Board at its next meeting.

DISTRIBUTION LIST

Copies of this Policy shall be maintained by:

- Board of Directors;
- Executive Director;
- Administration Department;
- Human Resources Unit;
- ICT Unit;
- Finance Department;
- Programme Department;
- MEAL Unit;
- Legal Unit;
- All Field Offices;
- Electronic Document Management System; and
- Official Policy Repository.

Every employee shall have access to the current approved version of this Policy.

LIST OF ABBREVIATIONS

Abbreviation	Meaning
AI	Artificial Intelligence
Board	Board of Directors
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
HR	Human Resources
ICT	Information and Communication Technology
ILA	Initiative for Legal Aid
IT	Information Technology
MEAL	Monitoring, Evaluation, Accountability and Learning
MFA	Multi-Factor Authentication
NGO	Non-Governmental Organization
PII	Personally Identifiable Information
PSEA	Protection from Sexual Exploitation and Abuse
SOP	Standard Operating Procedure
VPN	Virtual Private Network

TABLE OF CONTENETS

CHAPTER ONE
INTRODUCTION

1.8 Relationship with Other ILA Policies

CHAPTER TWO
DATA PROTECTION GOVERNANCE FRAMEWORK

2.1 Introduction

GUIDING PRINCIPLES OF DATA PROTECTION

2.2 General Principles

2.3 Principle of Lawfulness

2.4 Principle of Fairness

2.5 Principle of Transparency

2.6 Principle of Purpose Limitation

2.7 Principle of Data Minimization

2.8 Principle of Accuracy

2.9 Principle of Storage Limitation

2.10 Principle of Integrity

2.11 Principle of Confidentiality

2.12 Principle of Security

2.13 Principle of Accountability

2.14 Principle of Privacy by Design

2.15 Principle of Privacy by Default

2.16 Principle of Human Dignity and Respect

2.17 Principle of Do No Harm

DATA PROTECTION GOVERNANCE STRUCTURE

2.18 Purpose of the Governance Structure

2.40 Organizational Accountability

PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

2.41 General Principle

2.42 Privacy by Design

2.43 Privacy by Default

2.44 Privacy in Procurement and System Acquisition

DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

2.45 Purpose

2.46 Circumstances Requiring a DPIA

2.47 Contents of a DPIA

2.48 Review of DPIAs

INFORMATION GOVERNANCE RISK MANAGEMENT

2.49 Integration with Organizational Risk Management

2.50 Categories of Information Risk

2.51 Information Risk Assessments

REPORTING, MONITORING AND CONTINUOUS IMPROVEMENT

2.52 Internal Reporting

2.53 Monitoring and Assurance

2.54 Corrective and Preventive Actions

2.55 Continuous Improvement

CHAPTER THREE

CATEGORIES OF PERSONAL DATA AND DATA PROCESSING ACTIVITIES

3.1 Introduction

PERSONAL DATA

3.2 Meaning of Personal Data
3.3 Categories of Personal Data Processed by ILA
- A. Identification Information
- B. Contact Information
- C. Demographic Information
- D. Employment Information
- E. Financial Information
- F. Digital Information

3.3A Categories of Data Subjects

SPECIAL CATEGORIES OF PERSONAL DATA

3.4 General
3.5 Health Information
3.6 Safeguarding Information
3.7 Children's Personal Data
3.8 Criminal Justice Information
3.8A Genetic and Genetic-Related Information

LEGAL AID INFORMATION

3.9 Client Information
3.10 Legal Professional Privilege
3.11 Witness Information

HUMAN RESOURCE INFORMATION

3.12 Personnel Records
3.13 Recruitment Information

PROGRAMME, BENEFICIARY AND COMMUNITY INFORMATION

3.14 Beneficiary Information
3.15 Community Engagement Information
3.16 Complaints and Feedback Information

DONOR, PARTNER AND STAKEHOLDER INFORMATION

3.17 Donor Information
3.18 Partner Information

RESEARCH, MONITORING, EVALUATION, ACCOUNTABILITY AND LEARNING (MEAL)

3.19 Research Information
3.20 MEAL Information

DIGITAL INFORMATION AND ELECTRONIC COMMUNICATIONS

3.21 Electronic Communications
3.22 Website Information
3.23 Social Media Information

AUDIO, VISUAL AND BIOMETRIC INFORMATION

3.24 Photographs
3.25 Audio and Video Recordings
3.26 CCTV
3.27 Biometric Information

ANONYMIZATION, PSEUDONYMIZATION AND AGGREGATION

3.28 Anonymized Data
3.29 Pseudonymized Data
3.30 Aggregated Data
3.30A De-identification Techniques

DATA CLASSIFICATION FRAMEWORK

3.31 Purpose
3.32 Classification Levels
  A. Public Information
  B. Internal Information
  C. Confidential Information
  D. Highly Confidential Information
3.33 Classification Responsibilities
3.34 Review of Information Classification

CHAPTER FOUR

LAWFUL BASES FOR PROCESSING PERSONAL DATA

4.1 Purpose

GENERAL PRINCIPLES

4.2 Requirement for a Lawful Basis
4.3 Necessity and Proportionality
4.3A Lawful Basis Register

CONSENT

4.4 Processing Based on Consent
4.5 Obtaining Consent
4.6 Withdrawal of Consent
4.7 Situations Where Consent Is Not Required

PERFORMANCE OF A CONTRACT

4.8 Contractual Necessity

COMPLIANCE WITH LEGAL OBLIGATIONS

4.9 Legal Obligations

PROTECTION OF VITAL INTERESTS

4.10 Vital Interests

LEGITIMATE ORGANIZATIONAL INTERESTS

4.11 Legitimate Interests
4.12 Legitimate Interest Assessment (LIA)
4.12A Data Protection Impact Assessments (DPIAs)

PROCESSING IN THE PUBLIC INTEREST AND HUMANITARIAN ACTIVITIES

4.13 Public Interest Processing
4.14 Humanitarian and Emergency Response

LEGAL PROCEEDINGS, LEGAL ADVICE, AND DISPUTE RESOLUTION

4.15 Processing for Legal Services
4.16 Litigation and Dispute Resolution

DIRECT COLLECTION FROM INDIVIDUALS

5.8 General Rule
5.9 Interviews and Client Consultations
5.10 Legal Aid Intake Information

COLLECTION FROM CHILDREN AND VULNERABLE PERSONS

5.11 Enhanced Protection Requirement
5.12 Child Data Collection
5.13 Vulnerable Individuals

COLLECTION FROM THIRD PARTIES

5.14 Indirect Collection
5.15 Requirements for Third-Party Collection
5.16 Information Received from Courts and Authorities

FIELD DATA COLLECTION

5.17 Field Operations
5.18 Mobile Data Collection

ELECTRONIC AND ONLINE DATA COLLECTION

5.19 Digital Collection Platforms
5.20 Online Forms and Electronic Questionnaires
5.21 Cookies and Website Technologies

CONSENT COLLECTION PROCEDURES

5.22 General Requirements for Consent
5.23 Written Consent
5.24 Verbal Consent
5.25 Consent for Images and Public Communications

COLLECTION OF PHOTOGRAPHS, AUDIO AND VIDEO RECORDINGS

5.26 General Requirements
5.27 Images of Children and Vulnerable Persons

COLLECTION FOR RESEARCH AND MEAL ACTIVITIES

5.28 Ethical Data Collection
5.29 Surveys and Assessments

COLLECTION THROUGH HUMAN RESOURCES PROCESSES

5.30 Recruitment Data Collection
5.31 Employee Records Collection

COLLECTION THROUGH COMPLAINTS AND INVESTIGATIONS

5.32 Complaints Information
5.33 Investigation Information

DATA COLLECTION DOCUMENTATION

5.34 Data Collection Records
5.35 Review of Collection Practices

PROHIBITED DATA COLLECTION PRACTICES

5.36 Prohibited Collection Activities

CHAPTER SIX

DATA STORAGE, SECURITY AND ACCESS CONTROL

6.1 Introduction

GENERAL DATA SECURITY PRINCIPLES

6.2 Security Obligations
6.3 Confidentiality, Integrity and Availability
6.4 Security by Risk-Based Approach

PHYSICAL STORAGE SECURITY

6.5 Paper Records
6.6 Physical File Storage Requirements
6.7 Legal Files
6.8 Transport of Physical Records

ELECTRONIC STORAGE SECURITY

6.9 Electronic Information Systems
6.10 Prohibited Electronic Storage

INFORMATION SECURITY CONTROLS

6.11 Access Control
6.12 Role-Based Access Control
6.13 User Accounts
6.14 Access Review

PASSWORD AND AUTHENTICATION SECURITY

6.15 Password Requirements
6.16 Multi-Factor Authentication

ENCRYPTION AND SECURE TRANSMISSION

6.17 Encryption
6.18 Transmission of Personal Data
6.19 Email Security

BACKUP AND BUSINESS CONTINUITY

6.20 Data Backup
6.21 Backup Requirements
6.22 Disaster Recovery

DEVICE SECURITY AND REMOTE WORKING

6.23 Organizational Devices
6.24 Personal Devices
6.25 Mobile Devices
6.26 Lost or Stolen Devices

REMOTE WORK AND OFF-SITE ACCESS

6.27 Remote Working Arrangements
6.28 Public Networks

CLOUD STORAGE AND THIRD-PARTY PLATFORMS

6.29 Use of Cloud Services
6.30 Approved Platforms
6.31 Third-Party Service Providers

ACCESS LOGGING AND MONITORING

6.32 Access Monitoring
6.33 Purpose of Monitoring
6.34 Review of Access Records

CONFIDENTIALITY OBLIGATIONS

6.35 Duty of Confidentiality
6.36 Confidentiality Agreements
6.37 Professional Confidentiality

STAFF RESPONSIBILITIES FOR DATA SECURITY

6.38 Responsibilities of All Personnel
6.39 Responsibilities of Managers
6.40 Responsibilities of ICT Unit

SECURITY TRAINING AND AWARENESS

6.41 Training Requirements
6.42 Periodic Awareness Activities

REVIEW AND IMPROVEMENT OF SECURITY CONTROLS

6.43 Security Reviews
6.44 Corrective Measures
6.45 Continuous Improvement

CHAPTER SEVEN

DATA SHARING, DISCLOSURE AND TRANSFER OF PERSONAL DATA

7.1 Introduction

GENERAL PRINCIPLES FOR DATA SHARING

7.2 Data Sharing Principles
7.3 Authorization Before Sharing

INTERNAL DATA SHARING

7.4 Sharing Between Departments
7.5 Need-to-Know Principle
7.6 Internal Restrictions

SHARING WITH EXTERNAL PARTIES

7.7 General Rule
7.8 Due Diligence Before External Sharing

DATA SHARING AGREEMENTS

7.9 Requirement for Agreements
7.10 Partner Organizations

DISCLOSURE TO GOVERNMENT AUTHORITIES AND COURTS

7.11 Government Requests
7.12 Court Orders

LEGAL PROFESSIONAL PRIVILEGE AND CONFIDENTIALITY

7.13 Protection of Legal Information
7.14 Client Consent for Disclosure

SAFEGUARDING AND PROTECTION-RELATED DISCLOSURES

7.15 Safeguarding Exceptions
7.16 Minimum Necessary Disclosure

DONOR AND PUBLIC REPORTING

7.17 Donor Reporting
7.18 Public Communications

RESEARCH, ACADEMIC AND POLICY DATA SHARING

7.19 Research Data Sharing
7.20 Academic Collaborations

SERVICE PROVIDERS AND DATA PROCESSORS

7.21 Use of Data Processors
7.22 Processor Obligations
7.23 Vendor Due Diligence

CROSS-BORDER TRANSFER OF PERSONAL DATA

7.24 General Principle
7.25 Assessment Before Transfer
7.26 Safeguards for International Transfers
7.27 High-Risk Transfers

8.9 Identity Verification
8.10 Access to Legal Files

RIGHT TO CORRECTION

8.11 Right to Rectification
8.12 Accuracy of Legal Records

RIGHT TO DELETION OR ERASURE

8.13 Right to Request Deletion
8.14 Limitations on Deletion
8.15 Secure Disposal Following Approval

RIGHT TO RESTRICT PROCESSING

8.16 Restriction Requests
8.17 Effect of Restriction

RIGHT TO OBJECT

8.18 Right to Object
8.19 Assessment of Objections

RIGHTS RELATING TO AUTOMATED DECISION-MAKING AND PROFILING

8.20 Automated Decision-Making
8.21 Automated Profiling

RIGHTS OF CLIENTS, BENEFICIARIES AND VULNERABLE PERSONS

8.22 Enhanced Protection for Vulnerable Individuals
8.23 Legal Aid Client Rights
8.24 Beneficiary Rights

AUTHORIZED REPRESENTATIVES

8.25 Requests Through Representatives
8.26 Verification of Representatives
8.27 Children and Persons Lacking Capacity

REQUEST SUBMISSION AND MANAGEMENT PROCEDURE

8.28 Submission of Requests
8.29 Minimum Information Required
8.30 Request Registration

RESPONSE TIMELINES

8.31 Timely Response
8.32 Extension of Time

FEES AND COSTS

8.33 No Unreasonable Charges
8.34 Exceptional Administrative Costs

REFUSAL OR RESTRICTION OF REQUESTS

8.35 Grounds for Refusal
8.36 Communication of Refusal

COMPLAINTS AND APPEALS MECHANISM

8.37 Right to Complain
8.38 Internal Review
8.39 Independent Review

PROTECTION AGAINST RETALIATION

8.40 Non-Retaliation Principle
8.41 Confidential Handling of Requests

RECORD KEEPING AND CONTINUOUS IMPROVEMENT

8.42 Data Subject Request Records
8.43 Monitoring and Improvement

CHAPTER NINE

DATA PROTECTION GOVERNANCE AND RESPONSIBILITIES

9.1 Introduction

DATA PROTECTION GOVERNANCE FRAMEWORK

9.2 Governance Structure
9.3 Accountability Principle

BOARD OF DIRECTORS RESPONSIBILITIES

9.4 Role of the Board
9.5 Responsibilities of the Board

EXECUTIVE DIRECTOR RESPONSIBILITIES

9.6 Role of Executive Director
9.7 Responsibilities of Executive Director

DATA PROTECTION OFFICER

9.8 Appointment of Data Protection Officer
9.9 Responsibilities of Data Protection Officer
9.10 Independence of Data Protection Officer

LEGAL DEPARTMENT RESPONSIBILITIES

9.11 Role of Legal Department
9.12 Legal Department Duties

ICT UNIT RESPONSIBILITIES

9.13 Role of ICT Unit
9.14 ICT Responsibilities

HUMAN RESOURCES DEPARTMENT RESPONSIBILITIES

9.15 Role of Human Resources
9.16 HR Responsibilities

PROGRAMME DEPARTMENT RESPONSIBILITIES

9.17 Programme Data Responsibilities

MEAL UNIT RESPONSIBILITIES

9.18 MEAL Data Protection Responsibilities
9.19 MEAL Duties

SAFEGUARDING UNIT RESPONSIBILITIES

9.20 Safeguarding Data Protection Responsibilities
9.21 Safeguarding Duties

FINANCE AND ADMINISTRATION DEPARTMENT RESPONSIBILITIES

9.22 Role of Finance and Administration Department
9.23 Finance and Administration Duties

RECORDS MANAGEMENT RESPONSIBILITIES

9.24 Role of Records Management Function
9.25 Records Management Duties

DEPARTMENTAL DATA OWNERS

9.26 Appointment of Data Owners
9.27 Responsibilities of Data Owners

RESPONSIBILITIES OF ALL STAFF AND AFFILIATED PERSONNEL

9.28 General Responsibility
9.29 Staff Obligations

VOLUNTEERS, INTERNS AND CONSULTANTS

9.30 Extended Personnel Obligations
9.31 Contractual Requirements

PARTNER AND THIRD-PARTY RESPONSIBILITIES

9.32 Responsibilities of Partners
9.33 Partner Obligations

DATA PROTECTION COMMITTEE

9.34 Establishment of Data Protection Committee
9.35 Composition of Committee
9.36 Responsibilities of Data Protection Committee

REPORTING STRUCTURES

9.37 Data Protection Reporting
9.38 Significant Matters

GOVERNANCE REVIEW AND CONTINUOUS IMPROVEMENT

9.39 Periodic Governance Review
9.40 Continuous Improvement

CHAPTER TEN

DATA PROTECTION COMPLIANCE, AUDIT AND MONITORING

10.1 Introduction

DATA PROTECTION COMPLIANCE FRAMEWORK

10.2 Compliance Commitment
10.3 Compliance Principles

DATA PROTECTION COMPLIANCE MONITORING

10.4 Purpose of Monitoring
10.5 Monitoring Activities
10.6 Departmental Compliance Reviews

DATA PROTECTION AUDITS

10.7 Purpose of Audits
10.8 Types of Audits
10.9 Audit Frequency

AUDIT PROCESS

10.10 Audit Planning
10.11 Audit Evidence
10.12 Audit Findings Classification

CORRECTIVE ACTION AND IMPROVEMENT

10.13 Corrective Action Plans
10.14 Priority of Corrective Actions
10.15 Follow-Up Reviews

COMPLIANCE REPORTING

10.16 Data Protection Reports
10.17 Management Reporting
10.18 Serious Compliance Issues

DATA PROTECTION PERFORMANCE INDICATORS

10.19 Compliance Indicators
10.20 Use of Performance Information

STAFF COMPLIANCE MONITORING

10.21 Purpose of Staff Compliance Monitoring
10.22 Methods of Staff Compliance Monitoring
10.23 Performance Management Integration

TRAINING COMPLIANCE MONITORING

10.24 Training Requirements
10.25 Training Monitoring
10.26 Additional Training Requirements

THIRD-PARTY COMPLIANCE MONITORING

10.27 Monitoring Third Parties
10.28 Third-Party Compliance Measures
10.29 Third-Party Non-Compliance

DONOR AND PARTNER COMPLIANCE REQUIREMENTS

10.30 Donor Compliance
10.31 Partner Compliance Reviews

RECORDS OF PROCESSING ACTIVITIES

10.32 Establishment of Processing Records
10.33 Contents of Processing Records
10.34 Review of Processing Records

DATA PROTECTION COMPLIANCE REGISTER

10.35 Establishment of Compliance Register
10.36 Contents of Compliance Register
10.37 Purpose of Compliance Register

MANAGEMENT REVIEW OF DATA PROTECTION FRAMEWORK

10.38 Management Review
10.39 Matters for Review
10.40 Outcomes of Management Review

CONTINUOUS IMPROVEMENT FRAMEWORK

10.41 Commitment to Improvement
10.42 Lessons Learned
10.43 Review of Policy Effectiveness

CHAPTER ELEVEN

DATA PROTECTION TRAINING, AWARENESS AND ORGANIZATIONAL CULTURE

11.1 Introduction

DATA PROTECTION CULTURE

11.2 Commitment to Privacy Culture
11.3 Principles of Organizational Data Protection Culture

TRAINING REQUIREMENTS

11.4 Mandatory Training
11.5 Timing of Training

STAFF INDUCTION TRAINING

11.6 Data Protection Induction
11.7 Induction Topics

SPECIALIZED TRAINING PROGRAMMES

11.8 Legal Staff Training
11.9 Safeguarding Personnel Training
11.10 ICT Personnel Training
11.11 MEAL and Research Personnel Training
11.12 Finance and HR Personnel Training

AWARENESS PROGRAMMES

11.13 Awareness Activities
11.14 Key Awareness Messages

CONFIDENTIALITY COMMITMENTS

11.15 Confidentiality Agreements
11.16 Continuing Confidentiality Obligations

TRAINING ASSESSMENT AND EFFECTIVENESS

11.17 Evaluation of Training
11.18 Improving Training Programmes

TRAINING RECORD MANAGEMENT

11.19 Training Records
11.20 Monitoring Training Compliance

PARTNER, CONTRACTOR AND THIRD-PARTY AWARENESS

11.21 Awareness Requirements for External Persons
11.22 External Awareness Measures
11.23 Partner Compliance Confirmation

BOARD AND GOVERNANCE AWARENESS

11.24 Board Data Protection Awareness
11.25 Executive Management Awareness

DATA PROTECTION CHAMPIONS

11.26 Establishment of Data Protection Champions
11.27 Role of Data Protection Champions
11.28 Selection of Champions

PRIVACY COMMUNICATION STRATEGY

11.29 Purpose of Communication
11.30 Communication Channels
11.31 Communication Topics

TRAINING RESPONSIBILITIES

11.32 Role of Human Resources Department
11.33 Role of Data Protection Officer
11.34 Role of Department Heads

NON-COMPLIANCE WITH TRAINING REQUIREMENTS

11.35 Failure to Complete Required Training
11.36 Unauthorized Access Due to Training Failure

CONTINUOUS LEARNING FRAMEWORK

11.37 Commitment to Continuous Learning
11.38 Lessons Learned Approach
11.39 Annual Training Review

CHAPTER TWELVE

DATA PROTECTION INCIDENT RESPONSE AND BREACH MANAGEMENT

12.1 Introduction

DATA PROTECTION INCIDENTS

12.2 Definition of a Data Protection Incident
12.3 Examples of Data Protection Incidents

INCIDENT RESPONSE PRINCIPLES

12.4 Response Principles

INCIDENT IDENTIFICATION AND REPORTING

12.5 Duty to Report Incidents
12.6 Reporting Channels
12.7 Information Required in Incident Reports

IMMEDIATE RESPONSE ACTIONS

12.8 Initial Response
12.9 Containment Measures

INCIDENT CLASSIFICATION

12.10 Purpose of Classification
12.11 Incident Categories

- Level One: Minor Incident
- Level Two: Moderate Incident
- Level Three: Serious Incident
- Level Four: Critical Incident

INCIDENT INVESTIGATION

12.12 Investigation Process
12.13 Investigation Team
12.14 Investigation Confidentiality

BREACH RISK ASSESSMENT

12.15 Assessment Factors
12.16 Special Considerations

DATA BREACH NOTIFICATION PROCEDURES

12.17 Purpose of Notification
12.18 Internal Notification
12.19 External Notification

COMMUNICATION WITH AFFECTED PERSONS

12.20 Notification Principles
12.21 Content of Notifications
12.22 Protection-Sensitive Communication

CORRECTIVE AND REMEDIAL MEASURES

12.23 Immediate Remedial Actions
12.24 Long-Term Corrective Actions

ROOT CAUSE ANALYSIS

12.25 Purpose of Root Cause Analysis
12.26 Areas of Analysis
12.27 Root Cause Report

POST-INCIDENT REVIEW AND LESSONS LEARNED

12.28 Post-Incident Review
12.29 Lessons Learned Integration

DATA BREACH REGISTER

12.30 Establishment of Breach Register
12.31 Contents of Breach Register
12.32 Purpose of Breach Register

RESPONSIBILITIES FOR INCIDENT MANAGEMENT

12.33 Responsibilities of All Personnel
12.34 Responsibilities of Data Protection Officer
12.35 Responsibilities of ICT Unit
12.36 Responsibilities of Legal Department
12.37 Responsibilities of Safeguarding Unit

ANNEX: DATA BREACH INCIDENT REPORT TEMPLATE

12.38 Incident Report Structure

Section One: Incident Details

- Incident reference number
- Date and time
- Location
- Reporting person
- Department involved

Section Two: Description of Incident

- What happened
- How it occurred
- Information affected
- Systems or records involved

Section Three: Risk Assessment

- Persons affected
- Sensitivity of information
- Potential harm
- Risk level

Section Four: Response Actions

- Immediate containment
- Investigation actions
- Notifications
- Corrective measures

Section Five: Closure Review

- Root cause
- Lessons learned
- Preventive actions
- Responsible persons
- Completion date

CHAPTER THIRTEEN

DATA RETENTION, ARCHIVING AND SECURE DISPOSAL

13.1 Introduction

DATA RETENTION PRINCIPLES

13.2 Retention Principle
13.3 Data Minimization and Retention
13.4 Retention Factors

RECORD CATEGORIES AND RETENTION REQUIREMENTS

13.5 Legal Aid and Case Files
13.6 Retention of Legal Files
13.7 Confidentiality of Closed Case Files

BENEFICIARY AND PROGRAMME RECORDS

13.8 Programme Records
13.9 Retention of Beneficiary Information
13.10 Anonymization of Programme Data

SAFEGUARDING RECORDS

13.11 Protection of Safeguarding Information
13.12 Retention of Safeguarding Records
13.13 Destruction of Safeguarding Records

HUMAN RESOURCES RECORDS

13.14 Employee Records
13.15 Retention of HR Records

FINANCIAL AND PROCUREMENT RECORDS

13.16 Financial Records
13.17 Retention of Financial Records

DIGITAL ARCHIVING

13.18 Digital Archives
13.19 Digital Archive Controls

RECORD RETENTION SCHEDULE

13.20 Establishment of Retention Schedule
13.21 Review of Retention Schedule

SECURE DISPOSAL OF PERSONAL DATA

13.22 Purpose of Secure Disposal
13.23 Disposal Principles

PHYSICAL RECORD DESTRUCTION

13.24 Physical Documents
13.25 Approved Destruction Methods
13.26 Prohibited Disposal Practices

DIGITAL DATA DELETION

13.27 Digital Records Disposal
13.28 Digital Deletion Methods
13.29 Disposal of ICT Equipment

DISPOSAL AUTHORIZATION PROCEDURES

13.30 Approval Before Disposal
13.31 Disposal Approval Process
13.32 Authorized Approving Officers

LEGAL HOLD AND PRESERVATION REQUIREMENTS

13.33 Legal Hold
13.34 Management of Legal Holds

DISPOSAL RECORDS AND REGISTERS

13.35 Disposal Register
13.36 Contents of Disposal Register
13.37 Disposal Evidence

ARCHIVING RESPONSIBILITIES

13.38 Records Management Responsibility
13.39 Data Protection Officer Responsibilities
13.40 Legal Department Responsibilities
13.41 ICT Department Responsibilities

RETENTION AND DISPOSAL REGISTER TEMPLATE

13.42 Data Retention and Disposal Register

CHAPTER FOURTEEN

DATA PROTECTION GOVERNANCE STRUCTURE AND RESPONSIBILITIES

14.1 Introduction

DATA PROTECTION GOVERNANCE PRINCIPLES

14.2 Accountability Principle
14.3 Governance Principles

BOARD OF DIRECTORS OVERSIGHT

14.4 Role of the Board
14.5 Board Responsibilities
14.6 Board Confidentiality Obligations

EXECUTIVE DIRECTOR RESPONSIBILITIES

14.7 Executive Accountability
14.8 Responsibilities of Executive Director

DATA PROTECTION OFFICER

14.9 Appointment of Data Protection Officer
14.10 Role of Data Protection Officer
14.11 Responsibilities of Data Protection Officer

LEGAL DEPARTMENT RESPONSIBILITIES

14.12 Role of Legal Department
14.13 Legal Department Responsibilities

ICT DEPARTMENT RESPONSIBILITIES

14.14 Role of ICT Department
14.15 ICT Responsibilities

HUMAN RESOURCES DEPARTMENT RESPONSIBILITIES

14.16 Role of HR Department
14.17 HR Responsibilities

PROGRAMME DEPARTMENT RESPONSIBILITIES

14.18 Role of Programme Departments
14.19 Programme Responsibilities

MEAL DEPARTMENT RESPONSIBILITIES

14.20 Role of MEAL Unit
14.21 MEAL Responsibilities

SAFEGUARDING UNIT RESPONSIBILITIES

14.22 Role of Safeguarding Unit
14.23 Safeguarding Responsibilities

DEPARTMENTAL DATA OWNERS AND INFORMATION ASSET OWNERS

14.24 Appointment of Data Owners
14.25 Responsibilities of Data Owners
14.26 Information Asset Owners

RESPONSIBILITIES OF ALL STAFF AND PERSONNEL

14.27 General Staff Responsibility
14.28 Staff Obligations
14.29 Prohibited Staff Conduct

VOLUNTEER, INTERN AND CONSULTANT RESPONSIBILITIES

14.30 Application of Policy
14.31 Obligations of Non-Employees

PARTNER RESPONSIBILITIES

14.32 Partner Accountability
14.33 Partner Obligations

DATA PROTECTION COMMITTEE

14.34 Establishment of Data Protection Committee
14.35 Composition of Committee
14.36 Functions of Data Protection Committee
14.37 Committee Meetings

DATA PROTECTION REPORTING STRUCTURE

14.38 Reporting Lines
14.39 Regular Reporting
14.40 Serious Matter Reporting

GOVERNANCE REVIEW AND CONTINUOUS IMPROVEMENT

14.41 Periodic Governance Review
14.42 Review Considerations
14.43 Amendment of Governance Arrangements

CHAPTER FIFTEEN

DATA PROTECTION RISK MANAGEMENT AND COMPLIANCE MONITORING

15.1 Introduction

DATA PROTECTION RISK MANAGEMENT FRAMEWORK

15.2 Purpose of Risk Management
15.3 Risk Management Principles

IDENTIFICATION OF DATA PROTECTION RISKS

15.4 Sources of Privacy Risks
15.5 Categories of Data Protection Risks

DATA PROTECTION RISK ASSESSMENT

15.6 Risk Assessment Process
15.7 Risk Assessment Criteria
15.8 Risk Ratings

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

15.9 Purpose of DPIA
15.10 Situations Requiring DPIA
15.11 DPIA Contents
15.12 DPIA Responsibilities

DATA PROTECTION RISK REGISTER

15.13 Establishment of Risk Register
15.14 Contents of Risk Register
15.15 Risk Monitoring

COMPLIANCE MONITORING FRAMEWORK

15.16 Purpose of Compliance Monitoring
15.17 Compliance Monitoring Activities

INTERNAL DATA PROTECTION AUDITS

15.18 Purpose of Internal Audits
15.19 Scope of Data Protection Audits
15.20 Audit Frequency
15.21 Audit Independence

DATA PROTECTION COMPLIANCE ASSESSMENTS

15.22 Compliance Assessments
15.23 Areas of Assessment
15.24 Assessment Reports

CORRECTIVE ACTION MANAGEMENT

15.25 Corrective Action Plans
15.26 Contents of Corrective Action Plans
15.27 Monitoring Corrective Actions
15.28 Escalation of Outstanding Risks

DATA PROTECTION PERFORMANCE INDICATORS

15.29 Purpose of Indicators
15.30 Suggested Data Protection Indicators

MANAGEMENT REPORTING

15.31 Data Protection Reports
15.32 Contents of Reports
15.33 Reporting to the Board

DATA PROTECTION PERFORMANCE REVIEW

15.34 Annual Review
15.35 Review Areas
15.36 Outcomes of Review

CONTINUOUS IMPROVEMENT FRAMEWORK

15.37 Commitment to Improvement
15.38 Lessons Learned

COMPLIANCE MONITORING TOOLS AND TEMPLATES

15.39 Compliance Tools

- Annex I: Data Protection Risk Assessment Template
- Annex II: Data Protection Risk Register Template
- Annex III: Data Protection Impact Assessment Template
- Annex IV: Data Protection Audit Checklist
- Annex V: Corrective Action Tracking Form
- Annex VI: Data Protection Compliance Review Report Template
- Annex VII: Annual Data Protection Performance Report Template

CHAPTER SIXTEEN

DATA PROTECTION POLICY IMPLEMENTATION, REVIEW AND AMENDMENT

16.1 Introduction

POLICY IMPLEMENTATION FRAMEWORK

16.2 Implementation Commitment
16.3 Implementation Responsibility
16.4 Operationalization of the Policy

POLICY OWNERSHIP

16.5 Policy Owner
16.6 Technical Ownership

POLICY APPROVAL AND EFFECTIVE DATE

16.7 Approval Authority
16.8 Effective Date
16.9 Binding Nature

POLICY COMMUNICATION AND ACCESSIBILITY

16.10 Communication of Policy
16.11 Accessibility of Policy

POLICY REVIEW

16.12 Periodic Review Requirement
16.13 Review Frequency
16.14 Circumstances Requiring Earlier Review

POLICY AMENDMENT PROCEDURES

16.15 Authority to Amend
16.16 Amendment Process
16.17 Documentation of Amendments

VERSION CONTROL

16.18 Policy Version Management
16.19 Version Control Information
16.20 Withdrawal of Previous Versions

POLICY EXCEPTIONS

16.21 Requests for Exceptions
16.22 Approval of Exceptions
16.23 Recording Exceptions

INTERPRETATION AND GUIDANCE

16.24 Interpretation Authority
16.25 Conflict with Other Policies
16.26 Alignment with Other Policies

FINAL PROVISIONS

16.27 Commitment to Privacy Protection
16.28 Compliance Obligation
16.29 Entry into Force

CHAPTER ONE

INTRODUCTION

1.1 Background

The Initiative for Legal Aid (ILA) is committed to promoting access to justice, the rule of law, human rights, and accountable governance through the provision of legal aid services, legal representation, legal empowerment, public interest litigation, policy advocacy, research, civic education, and community engagement.

In carrying out its mandate, ILA routinely collects, receives, generates, stores, processes, shares, and retains significant volumes of information relating to individuals and organizations. Such information includes, but is not limited to, personal data of beneficiaries, legal aid clients, survivors of human rights violations, children, vulnerable persons, witnesses, staff members, volunteers, interns, consultants, donors, partners, contractors, suppliers, and members of the public.

Many of the categories of information processed by ILA are highly confidential and sensitive. They include legal case files, court documents, witness statements, medical information, psychosocial assessments, financial records, employment records, safeguarding reports, complaints, disciplinary records, monitoring and evaluation data, photographs, digital communications, and other information that, if improperly accessed, disclosed, altered, or destroyed, could expose individuals to harm, compromise legal proceedings, undermine public confidence, or damage the reputation and operations of the Organization.

The rapid expansion of digital technologies, cloud-based information systems, mobile communications, artificial intelligence tools, and electronic service delivery has significantly increased both the opportunities and risks associated with the management of personal information. Cybersecurity threats, unauthorized disclosures, identity theft, phishing attacks, ransomware, accidental loss of data, insider misuse, and improper information sharing present serious operational, legal, financial, and reputational risks to organizations entrusted with sensitive information.

As an organization founded on principles of justice, confidentiality, integrity, accountability, and respect for human dignity, ILA recognizes that protecting personal data is both a legal and ethical obligation. Every individual whose information is entrusted to the Organization has the right to expect that such information will be handled responsibly, securely, fairly, and with due regard to their privacy and fundamental rights.

This Policy therefore establishes a comprehensive framework governing the lawful collection, processing, storage, use, disclosure, transfer, retention, archiving, and disposal of personal data throughout the Organization. It integrates internationally recognized data protection principles with sound information governance practices appropriate to the operational context of South Sudan and the requirements of ILA's partners, donors, and stakeholders.

The Policy also reinforces ILA's commitment to confidentiality, professional ethics, legal privilege, safeguarding, and responsible stewardship of information assets. It provides clear

standards and responsibilities for all persons handling information on behalf of the Organization and seeks to foster a culture in which privacy and data protection are embedded into every aspect of organizational planning, programme implementation, service delivery, and decision-making.

Ultimately, the protection of personal data is essential to maintaining the trust of beneficiaries, preserving the integrity of legal aid services, ensuring compliance with applicable legal and contractual obligations, mitigating organizational risk, and advancing ILA's mission in a manner that respects the dignity, rights, and security of every individual.

1.2 Purpose

The purpose of this Policy is to establish a comprehensive institutional framework for the governance, protection, management, and responsible use of personal data and other confidential information processed by the Initiative for Legal Aid.

The Policy seeks to ensure that all personal data processed by the Organization is collected, used, stored, disclosed, retained, archived, and disposed of in a lawful, fair, transparent, secure, and accountable manner, consistent with applicable legal requirements, contractual obligations, professional standards, and internationally recognized principles of data protection.

Specifically, this Policy is intended to:

a. Establish uniform standards and procedures for the management of personal data throughout the Organization;

b. Safeguard the privacy, dignity, confidentiality, and rights of all individuals whose information is processed by ILA;

c. Strengthen organizational governance by integrating data protection into programme management, legal services, administration, finance, human resources, procurement, monitoring and evaluation, safeguarding, and information technology functions;

d. Protect sensitive legal aid records, client files, safeguarding information, personnel records, financial information, donor information, and other confidential organizational information from unauthorized access, disclosure, alteration, loss, misuse, or destruction;

e. Promote accountability, transparency, and responsible stewardship of information assets across all levels of the Organization;

f. Reduce legal, operational, financial, cybersecurity, and reputational risks associated with the processing of personal data;

g. Establish clear roles, responsibilities, and reporting obligations for all persons who process personal data on behalf of ILA;

h. Strengthen public confidence and stakeholder trust in the Organization's information management practices; and

i. Ensure continuous improvement in privacy governance through monitoring, training, periodic reviews, and the adoption of evolving best practices in data protection and information security.

1.3 Objectives

The overarching objective of this Policy is to establish a robust and comprehensive data protection and privacy framework that safeguards the rights of individuals while enabling the Initiative for Legal Aid (ILA) to effectively fulfil its mandate in a secure, lawful, accountable, and ethical manner.

The specific objectives of this Policy are to:

1.3.1 Protection of Personal Data

Protect all personal data processed by the Organization against unauthorized access, disclosure, alteration, destruction, accidental loss, theft, misuse, unlawful processing, or any other form of compromise.

1.3.2 Protection of Privacy Rights

Respect and protect the privacy, dignity, autonomy, and fundamental rights of all individuals whose personal information is processed by ILA, including beneficiaries, legal aid clients, survivors, witnesses, children, staff, volunteers, consultants, contractors, donors, and partners.

1.3.3 Establishment of Organizational Standards

Establish standardized policies, procedures, controls, and governance mechanisms governing the collection, processing, storage, sharing, retention, archiving, and disposal of personal information throughout the Organization.

1.3.4 Promotion of Accountability

Promote accountability by clearly defining the roles, responsibilities, reporting obligations, and oversight functions of the Board of Directors, Management, employees, volunteers, consultants, contractors, and third-party service providers in relation to personal data.

1.3.5 Compliance with Legal and Contractual Obligations

Ensure compliance with applicable laws, contractual obligations, donor requirements, ethical standards, professional obligations, and internationally recognized principles relating to privacy, confidentiality, cybersecurity, and data protection.

1.3.6 Strengthening Information Governance

Strengthen organizational governance by integrating privacy and data protection into strategic planning, programme implementation, legal aid service delivery, financial management, human resources, procurement, monitoring and evaluation, safeguarding, and digital transformation initiatives.

1.3.7 Protection of Sensitive Information

Provide enhanced safeguards for particularly sensitive categories of information, including:

- legal aid case files;
- court documents;
- witness information;
- survivor information;
- children's information;
- safeguarding records;
- health information;
- financial records;
- employment records;
- disciplinary records; and
- information protected by legal professional privilege or confidentiality obligations.

1.3.8 Risk Management

Reduce legal, financial, operational, cybersecurity, reputational, and strategic risks associated with the improper handling of information.

1.3.9 Promotion of Ethical Information Management

Promote a culture of integrity, professionalism, confidentiality, and ethical decision-making in the handling of personal information.

1.3.10 Enhancement of Public Trust

Strengthen public confidence in ILA by demonstrating responsible stewardship of information entrusted to the Organization.

1.3.11 Support for Digital Transformation

Promote secure innovation through the responsible adoption of digital technologies, cloud computing, artificial intelligence tools, electronic case management systems, and online service delivery while maintaining appropriate safeguards for privacy and information security.

1.3.12 Continuous Improvement

Establish mechanisms for ongoing monitoring, auditing, evaluation, learning, and continual improvement of ILA's data protection and privacy management systems.

1.4 Scope

1.4.1 Persons Covered

This Policy applies to every individual and entity that collects, accesses, receives, processes, stores, transmits, shares, or otherwise handles personal data on behalf of ILA, irrespective of the nature or duration of their engagement.

Without limitation, this Policy applies to:

a. members of the Board of Directors;

b. the Executive Director;

c. all permanent employees;

d. temporary employees;

e. consultants;

f. volunteers;

g. interns;

h. legal practitioners and legal aid officers;

i. programme staff;

j. finance personnel;

k. human resources personnel;

l. ICT personnel;

m. monitoring, evaluation, accountability and learning personnel;

n. researchers;

o. contractors;

p. suppliers;

q. service providers;

r. implementing partners;

s. consortium partners;

t. sub-grantees;

u. data processors;

v. outsourced service providers;

w. independent experts; and

x. every other person acting on behalf of ILA.

Each person covered by this Policy has an individual responsibility to protect personal data and comply with its requirements.

1.4.2 Information Covered

This Policy applies to all information processed by ILA regardless of:

- format;
- medium;
- method of storage;
- geographical location; or
- technology used.

This includes information stored in:

- paper files;
- filing cabinets;
- electronic databases;
- servers;
- laptops;
- desktop computers;
- tablets;
- mobile phones;
- removable media;
- cloud platforms;
- email systems;
- messaging applications used for official purposes;
- video conferencing platforms;
- document management systems;
- case management systems;

- accounting software;
- human resource information systems;
- donor management systems;
- websites;
- social media management platforms; and
- archived storage facilities.

1.4.3 Categories of Information

This Policy applies to all categories of personal information processed by ILA, including but not limited to:

A. Beneficiary Information

Including:

- names;
- identification documents;
- addresses;
- telephone numbers;
- photographs;
- socioeconomic information;
- vulnerability assessments;
- programme participation records;
- beneficiary registration forms; and
- accountability and feedback records.

B. Legal Aid Client Information

Including:

- client files;
- pleadings;
- witness statements;
- legal advice;
- litigation records;
- contracts;
- mediation records;
- legal correspondence;
- court judgments;
- evidence; and
- privileged communications.

C. Human Resource Information

Including:

- recruitment records;
- employment contracts;
- payroll records;
- disciplinary records;
- leave records;
- performance evaluations;
- pension records;
- medical information;
- emergency contacts;
- identification documents; and
- training records.

D. Financial Information

Including:

- banking information;
- payment records;
- procurement records;
- invoices;
- taxation records;
- donor expenditure records;
- audit documentation; and
- financial reports containing personal information.

E. Safeguarding Information

Including:

- safeguarding complaints;
- PSEA reports;
- survivor information;
- confidential investigations;
- child protection records;
- psychosocial assessments; and
- referral documentation.

F. Digital Information

Including:

- email communications;

- login credentials;
- audit logs;
- metadata;
- IP addresses;
- CCTV recordings;
- website analytics;
- electronic signatures;
- digital certificates; and
- system access records.

1.4.4 Activities Covered

This Policy governs every stage of the information lifecycle, including:

- collection;
- recording;
- organization;
- classification;
- storage;
- retrieval;
- consultation;
- analysis;
- modification;
- transmission;
- disclosure;
- publication;
- sharing;
- archiving;
- retention;
- anonymization;
- pseudonymization;
- destruction; and
- disposal.

1.4.5 Territorial Scope

This Policy applies to all personal data processed by or on behalf of ILA irrespective of whether such processing occurs:

- at the Head Office;
- at regional or field offices;
- during outreach activities;
- in courts or tribunals;
- at partner institutions;
- during community engagements;
- while staff are working remotely;

- while travelling;
- within South Sudan; or
- outside South Sudan where information is processed on behalf of the Organization.

The obligations established under this Policy continue to apply regardless of the physical location of the data or the individual processing it.

1.5 Application

1.5.1 General Application

Compliance with this Policy is mandatory.

Every person to whom this Policy applies shall comply fully with its provisions as a condition of employment, engagement, appointment, consultancy, partnership, volunteering, or service provision.

No person may disregard the requirements of this Policy on the basis of convenience, operational pressure, technological limitations, or customary practice.

1.5.2 Binding Effect

This Policy forms an integral part of the governance framework of ILA and shall be read together with:

- the Human Resource and Administration Manual;
- ICT Policy;
- Financial Policy;
- Procurement and Asset Management Policy;
- MEAL Policy;
- Safeguarding and PSEA Policy;
- Code of Conduct and Ethics Policy;
- Risk Management Policy;
- Records Management Policy (where applicable);
- Information Security Procedures;
- employment contracts;
- consultancy agreements;
- volunteer agreements; and
- confidentiality undertakings.

Where any contract, manual, guideline, or procedure imposes a higher standard of confidentiality or data protection than this Policy, the higher standard shall prevail to the extent of the inconsistency.

1.5.3 Obligation to Report Non-Compliance

Every person covered by this Policy has an affirmative duty to promptly report any actual, suspected, or attempted breach of this Policy, unauthorized disclosure of personal data, cybersecurity incident, loss of records, or other event that may compromise the confidentiality, integrity, or availability of information.

Failure to report such incidents may itself constitute misconduct and may result in disciplinary or contractual action.

1.6 POLICY STATEMENT

The Initiative for Legal Aid (ILA) recognizes that privacy is a fundamental human right and that the responsible management of personal data is essential to protecting the dignity, security, autonomy, and lawful interests of every individual with whom the Organization interacts.

As an organization dedicated to advancing access to justice, human rights, the rule of law, and accountable governance, ILA routinely processes significant volumes of personal and sensitive information in the course of delivering legal aid services, public interest litigation, legal empowerment programmes, research, advocacy, monitoring and evaluation, safeguarding, human resources management, finance, procurement, administration, and organizational governance.

The Organization acknowledges that the improper collection, use, disclosure, alteration, retention, or disposal of personal information may expose individuals to discrimination, identity theft, physical harm, financial loss, reputational damage, retaliation, psychological trauma, or violations of their legal rights. Such failures may also expose the Organization to legal liability, contractual sanctions, financial losses, cybersecurity risks, regulatory action, and loss of stakeholder confidence.

Accordingly, ILA is committed to ensuring that all personal data and confidential information under its control are processed in accordance with the highest standards of legality, fairness, transparency, accountability, integrity, confidentiality, and security.

The Organization shall implement appropriate administrative, technical, physical, contractual, and organizational safeguards designed to protect information throughout its lifecycle, from collection to final disposal.

In particular, ILA commits to:

a. Process personal data only for lawful, legitimate, specified, and documented purposes;

b. Collect only the minimum amount of personal information necessary to achieve legitimate organizational objectives;

c. ensure that personal information remains accurate, complete, relevant, and up to date;

d. Implement appropriate safeguards to protect information against unauthorized access, disclosure, destruction, alteration, loss, theft, misuse, cyberattack, accidental damage, or unlawful processing;

e. Maintain strict confidentiality over legal aid files, court records, safeguarding reports, personnel records, donor information, financial information, and all other confidential information entrusted to the Organization;

f. Respect the rights of individuals concerning their personal information, including rights relating to access, correction, deletion, restriction, objection, and lawful processing, subject to applicable legal and professional obligations;

g. Integrate privacy and data protection considerations into programme design, project implementation, procurement, information technology, monitoring and evaluation, research, communications, fundraising, and organizational decision-making;

h. Ensure that employees, volunteers, consultants, contractors, and partners understand and fulfil their responsibilities under this Policy;

i. Promote a culture of confidentiality, ethical information management, and responsible stewardship of organizational information assets;

j. Investigate promptly every suspected breach of personal data or confidentiality;

k. Take appropriate corrective, disciplinary, contractual, civil, or criminal action where violations occur; and

l. Continually improve its information governance systems through regular monitoring, audits, training, technological enhancement, and policy review.

The Board of Directors, Executive Director, senior management, and every person acting on behalf of ILA share collective responsibility for ensuring that this commitment is effectively implemented throughout the Organization.

1.7 LEGAL AND REGULATORY FRAMEWORK

1.7.1 General

This Policy is informed by the Constitution of the Republic of South Sudan, applicable national legislation, internationally recognized principles of privacy and data protection, contractual obligations owed to donors and partners, professional ethical standards applicable to legal practitioners, and accepted international humanitarian information management standards.

Where South Sudanese legislation does not specifically regulate a particular aspect of personal data protection, ILA shall apply internationally recognized good practices to the extent that they are consistent with applicable law and organizational obligations.

1.7.2 National Legal Framework

This Policy shall be interpreted and implemented consistently with applicable laws of the Republic of South Sudan, including, where relevant:

a. the **Constitution of the Republic of South Sudan, 2011 (as amended)**;

b. the **Labour Act, 2017**;

c. the **Non-Governmental Organizations Act, 2016**;

d. the **Evidence Act, 2006** (where applicable to confidentiality, documentary evidence, and admissibility);

e. the **Code of Civil Procedure Act, 2007**;

f. the **Code of Criminal Procedure Act, 2008**;

g. the **Penal Code Act, 2008**, particularly provisions relating to unauthorized disclosure, fraud, forgery, computer-related offences, theft, and criminal misuse of information;

h. applicable legislation governing electronic communications, cybercrime, financial reporting, taxation, employment, procurement, archives, access to information, and records management as enacted or amended from time to time; and

i. any regulations, directives, or lawful orders issued by competent public authorities that affect the processing of personal information.

1.7.3 International Standards and Good Practice

In implementing this Policy, ILA shall be guided, where appropriate, by internationally recognized standards and principles, including:

a. the **Universal Declaration of Human Rights**, particularly the right to privacy and protection against arbitrary interference;

b. the **International Covenant on Civil and Political Rights**;

c. the **African Charter on Human and Peoples' Rights**;

d. the **African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)**, where relevant as a best-practice framework;

e. the principles reflected in the **EU General Data Protection Regulation (GDPR)**, where required by contractual obligations or donor requirements, or where adopted by ILA as organizational best practice;

f. humanitarian data responsibility and information protection principles developed by international humanitarian organizations;

g. professional standards governing legal confidentiality and legal professional privilege; and

h. internationally recognized information security and privacy management standards, including relevant ISO standards adopted by the Organization from time to time.

1.7.4 Contractual Obligations

ILA recognizes that many donor agreements, partnership agreements, funding contracts, consultancy agreements, service contracts, and memoranda of understanding impose specific obligations relating to confidentiality, cybersecurity, privacy, safeguarding, and protection of personal information.

Where contractual obligations establish more stringent requirements than those contained in this Policy, the stricter contractual requirements shall prevail, provided they do not conflict with applicable law.

1.7.5 Professional and Ethical Obligations

All legal practitioners, legal aid officers, consultants, mediators, investigators, researchers, safeguarding personnel, counsellors, finance officers, human resource personnel, ICT personnel, and other professionals acting on behalf of ILA shall continue to observe any additional duties of confidentiality, professional privilege, or ethical conduct imposed by their respective professions, regulatory bodies, or professional codes of ethics.

Nothing in this Policy shall be interpreted as limiting legal professional privilege or any legally recognized duty of confidentiality.

1.8 RELATIONSHIP WITH OTHER ILA POLICIES

This Policy forms an integral component of ILA's governance, compliance, and risk management framework and shall be implemented in conjunction with all other organizational policies governing information management, accountability, ethics, safeguarding, security, and institutional governance.

Accordingly, this Policy shall be read together with, and where appropriate implemented alongside, the following organizational instruments:

- Human Resource and Administration Manual;
- ICT Policy;
- Information Security Procedures and Standards;
- Financial Policy;
- Procurement and Asset Management Policy;
- Risk Management Policy;

- Code of Conduct and Ethics Policy;
- Safeguarding and Protection from Sexual Exploitation and Abuse (PSEA) Policy;
- Monitoring, Evaluation, Accountability and Learning (MEAL) Policy;
- Complaints Handling and Feedback Policy;
- Anti-Fraud, Anti-Corruption and Whistleblowing Policy;
- Records and Document Management Policy (where adopted);
- Partnership Management Policy;
- Business Continuity and Disaster Recovery Policy;
- Child Protection Policy (where maintained separately); and
- any other governance instruments approved by the Board of Directors.

Where two or more organizational policies address the same subject matter, they shall be interpreted harmoniously to give effect to the objectives of each policy. In the event of any inconsistency concerning the protection of personal data or confidential information, the provision that affords the **higher standard of privacy, confidentiality, security, or legal protection** shall prevail, unless otherwise required by applicable law.

All departmental procedures, standard operating procedures (SOPs), manuals, templates, forms, digital systems, and operational guidelines developed under this Policy shall be consistent with its provisions and shall be reviewed periodically to ensure continued alignment with organizational objectives, legal developments, technological advancements, and emerging best practices.

CHAPTER TWO

DATA PROTECTION GOVERNANCE FRAMEWORK

2.1 Introduction

Effective protection of personal data requires more than technical safeguards or isolated compliance measures. It requires an organization-wide governance system that integrates privacy, confidentiality, accountability, information security, ethical decision-making, and risk management into every aspect of organizational operations.

ILA recognizes that personal data is a strategic organizational asset entrusted to the Organization by beneficiaries, legal aid clients, staff members, volunteers, donors, partners, suppliers, and members of the public. The Organization further recognizes that improper management of such information may compromise individual rights, undermine public confidence, expose vulnerable persons to harm, jeopardize legal proceedings, and create significant legal, operational, financial, and reputational risks.

Accordingly, ILA adopts a comprehensive data governance framework that establishes clear principles, institutional responsibilities, decision-making structures, operational controls, oversight mechanisms, and accountability processes to ensure that personal data is processed responsibly throughout its lifecycle.

The governance framework established under this Chapter shall apply across all programmes, departments, projects, field offices, digital platforms, information systems, and operational activities of the Organization.

PART I: GUIDING PRINCIPLES OF DATA PROTECTION

2.2 General Principles

All processing of personal data by or on behalf of ILA shall be guided by the following fundamental principles. These principles are mandatory and shall inform every decision relating to the collection, use, disclosure, storage, transfer, retention, archiving, and disposal of personal information.

No operational objective, programme requirement, funding consideration, technological convenience, or administrative practice shall justify departure from these principles except where expressly authorized by applicable law.

2.3 Principle of Lawfulness

ILA shall process personal data only where there exists a lawful and legitimate basis for doing so.

Personal data shall not be collected or processed arbitrarily, deceptively, excessively, or for purposes inconsistent with applicable law, contractual obligations, professional duties, or this Policy.

Before collecting personal information, the Organization shall identify and document the legal, contractual, operational, or ethical basis upon which the information is required.

All processing activities shall remain within the limits of the authority under which the information was obtained.

2.4 Principle of Fairness

Personal information shall be processed fairly and in a manner that respects the dignity, autonomy, and legitimate expectations of the individual concerned.

ILA shall not obtain information through fraud, coercion, intimidation, manipulation, or other unfair means except where lawful investigative processes expressly permit otherwise.

Individuals shall not be subjected to unjustified adverse treatment arising from the processing of their personal information.

2.5 Principle of Transparency

The Organization shall ensure that individuals understand:

- why their information is being collected;
- what information is being collected;
- how it will be used;
- who may access it;
- how long it will be retained;
- the safeguards applied to it;
- their rights regarding the information; and
- the procedures available for raising concerns or complaints.

Privacy notices, consent forms, beneficiary registration forms, employment documents, procurement documentation, legal aid intake forms, and digital platforms shall clearly communicate these matters using language that is understandable to the intended audience.

2.6 Principle of Purpose Limitation

Personal data shall be collected only for specific, explicit, legitimate, and documented purposes.

Information collected for one purpose shall not subsequently be used for an unrelated purpose unless:

a. additional lawful authority exists;

b. the individual has provided informed consent where appropriate;

c. another legal obligation requires the processing;

d. the new purpose is compatible with the original purpose; or

e. exceptional humanitarian, safeguarding, judicial, or public interest considerations justify such processing.

Programme teams shall avoid "function creep," whereby information collected for one purpose is gradually used for unrelated activities without proper authorization.

2.7 Principle of Data Minimization

ILA shall collect and process only the minimum amount of personal information necessary to achieve the identified purpose.

Departments shall avoid requesting unnecessary documentation or excessive personal details merely because they may be useful in the future.

Where anonymous, aggregated, pseudonymized, or de-identified information is sufficient for operational purposes, identifiable personal data should not be collected.

Programme forms, surveys, legal intake forms, employment forms, procurement documents, and digital systems shall be reviewed periodically to eliminate unnecessary data collection.

2.8 Principle of Accuracy

Reasonable measures shall be taken to ensure that personal information remains accurate, complete, relevant, current, and reliable.

Individuals shall be afforded reasonable opportunities to update inaccurate information.

Where information is discovered to be inaccurate, incomplete, misleading, duplicated, or obsolete, corrective action shall be taken without undue delay.

Departments shall establish procedures for periodic verification of critical records.

2.9 Principle of Storage Limitation

Personal information shall not be retained indefinitely.

Information shall be retained only for as long as necessary to fulfil:

- legal obligations;
- contractual obligations;
- operational requirements;
- donor requirements;
- audit requirements;
- litigation requirements;
- safeguarding obligations; or
- legitimate organizational purposes.

Upon expiry of the applicable retention period, records shall be securely archived, anonymized, or destroyed in accordance with the Records Retention Schedule and Secure Disposal Procedures established under this Policy.

2.10 Principle of Integrity

ILA shall maintain the integrity of personal information throughout its lifecycle.

Appropriate controls shall be implemented to protect information against:

- unauthorized alteration;
- accidental modification;
- corruption;

- deletion;
- falsification;
- manipulation; and
- unauthorized destruction.

Critical organizational records shall be protected through version control, audit trails, backup systems, and appropriate authorization procedures.

2.11 Principle of Confidentiality

Confidential information shall be accessible only to persons who require such information for legitimate organizational purposes.

Every individual processing personal information shall observe strict confidentiality both during and after their engagement with the Organization.

Confidentiality obligations continue even after employment, consultancy, volunteer service, or contractual relationships have ended.

The unauthorized disclosure of confidential information constitutes serious misconduct and may attract disciplinary, contractual, civil, or criminal consequences.

2.12 Principle of Security

ILA shall implement proportionate administrative, technical, physical, contractual, and organizational safeguards to protect information against foreseeable threats.

Security measures shall be risk-based and shall address:

- confidentiality;
- integrity;
- availability; and
- resilience of information systems.

Security controls shall evolve continually in response to emerging technologies, cyber threats, operational risks, and organizational needs.

2.13 Principle of Accountability

Every individual who processes personal information on behalf of ILA is personally accountable for complying with this Policy.

Accountability requires that decisions concerning personal data can be justified, documented, audited, and reviewed.

Management shall ensure that adequate governance structures, internal controls, reporting mechanisms, and monitoring systems are maintained to demonstrate compliance with this Policy.

Failure to comply with data protection obligations shall result in appropriate corrective and disciplinary action.

2.14 Principle of Privacy by Design

Privacy considerations shall be incorporated into the design, procurement, development, implementation, and review of all programmes, projects, information systems, digital platforms, technologies, databases, and operational procedures.

Data protection shall not be treated as an afterthought or addressed only after risks have materialized.

Every new initiative involving personal information shall undergo an assessment of potential privacy risks before implementation.

2.15 Principle of Privacy by Default

The default configuration of every information system, application, database, digital platform, or operational process shall ensure the highest practical level of privacy protection.

Unless a legitimate operational reason exists:

- access shall be restricted;
- information sharing shall be limited;
- unnecessary data fields shall be disabled;
- public visibility shall be minimized; and
- retention periods shall not exceed operational necessity.

2.16 Principle of Human Dignity and Respect

The processing of personal information shall always respect the dignity, autonomy, equality, and rights of every individual.

No person shall be subjected to discrimination, stigmatization, harassment, exploitation, retaliation, or unjust treatment arising from the collection or use of their personal information.

Special care shall be exercised where information concerns vulnerable or marginalized persons.

2.17 Principle of Do No Harm

ILA shall ensure that its information management practices do not expose individuals, communities, or organizations to avoidable risks.

Before collecting, using, sharing, or publishing personal information, the Organization shall assess whether such processing could reasonably result in:

- physical harm;
- psychological harm;
- social exclusion;
- retaliation;
- discrimination;
- legal prejudice;
- economic loss;
- reputational damage; or
- security threats.

Where such risks are identified, appropriate mitigation measures shall be implemented before processing proceeds.

2.18 Purpose of the Governance Structure

The purpose of the Data Protection Governance Structure is to ensure that responsibility for the protection of personal data is clearly allocated throughout the Organization and that appropriate oversight, accountability, decision-making, and reporting mechanisms exist at every organizational level.

Data protection shall not be regarded solely as an ICT function. Rather, it is a shared institutional responsibility requiring active participation by the Board of Directors, Management, programme teams, support departments, and every individual processing personal information on behalf of ILA.

The governance structure established under this Policy is intended to:

a. Promote leadership accountability for privacy and data protection;

b. Ensure consistent implementation of this Policy across all departments and programmes;

c. Facilitate effective decision-making regarding privacy risks and information governance;

d. Integrate data protection into organizational planning and risk management;

e. Strengthen oversight of information security and confidentiality; and

f. Foster a culture of responsible stewardship of information assets.

2.19 Data Protection Governance Hierarchy

Responsibility for data protection within ILA shall be exercised through the following governance hierarchy:

1. Board of Directors;
2. Executive Director;
3. Senior Management Team;
4. ICT Unit;
5. Human Resources Unit;
6. Legal Unit;
7. MEAL Unit;
8. Finance and Administration Department;
9. Programme Departments;
10. Project Managers and Team Leaders;
11. Employees and Volunteers;
12. Consultants and Contractors; and
13. Third-Party Data Processors and Service Providers.

Each level of the hierarchy shall exercise responsibilities appropriate to its authority and shall cooperate to ensure the effective implementation of this Policy.

2.20 Responsibilities of the Board of Directors

The Board of Directors bears ultimate responsibility for the governance of personal data within ILA.

Without prejudice to its broader governance responsibilities, the Board shall:

a. Approve this Policy and any substantive amendments thereto;

b. Establish the strategic direction for privacy and information governance within the Organization;

c. Ensure that adequate financial, human, technological, and organizational resources are allocated to support implementation of this Policy;

d. Oversee organizational compliance with applicable legal, contractual, and ethical obligations relating to data protection;

e. Review reports concerning significant data breaches, cybersecurity incidents, and major privacy risks;

f. Ensure that privacy risks are integrated into the Organization's enterprise risk management framework;

g. Promote a culture of accountability, confidentiality, and ethical information management;

h. Require Management to implement appropriate corrective actions where weaknesses are identified;

i. Receive periodic reports on the effectiveness of organizational data protection controls;

j. Monitor organizational preparedness to respond to emerging information security threats; and

k. Ensure that data protection remains an integral component of organizational governance.

The Board may delegate operational oversight to an appropriate Board Committee, but such delegation shall not relieve the Board of its ultimate accountability.

2.21 Responsibilities of the Executive Director

The Executive Director shall serve as the chief executive authority responsible for the implementation and enforcement of this Policy.

The Executive Director shall:

a. Ensure Organization-wide implementation of this Policy;

b. Promote a culture that values privacy, confidentiality, and responsible information management;

c. Allocate adequate financial, technological, and human resources for data protection;

d. Ensure that departmental procedures comply with this Policy;

e. Approve organizational information security initiatives;

f. Oversee the management of significant data protection risks;

g. Ensure that appropriate incident response mechanisms exist;

h. Authorize corrective measures following significant breaches;

i. Ensure regular staff training and awareness;

j. Report material privacy risks to the Board;

k. Ensure compliance with donor information protection obligations;

l. Approve organizational data sharing arrangements where required; and

m. Ensure periodic review of this Policy.

2.22 Responsibilities of the Senior Management Team

Senior Management shall ensure that privacy and data protection are integrated into strategic planning, operational management, programme implementation, budgeting, procurement, and organizational decision-making.

Senior Management shall:

a. Implement this Policy within their respective departments;

b. Identify privacy risks arising from departmental operations;

c. Ensure staff compliance;

d. Allocate departmental resources for compliance activities;

e. Monitor departmental implementation;

f. Review incident reports;

g. Ensure corrective actions are implemented promptly;

h. Supervise departmental record management;

i. Ensure appropriate staff training; and

j. Cooperate during audits, investigations, and compliance reviews.

2.23 Responsibilities of the ICT Unit

The ICT Unit serves as the primary technical custodian of ILA's information systems and digital infrastructure.

The ICT Unit shall:

a. Design, implement, and maintain appropriate technical safeguards for organizational information systems;

b. Ensure secure configuration of servers, networks, databases, cloud services, endpoints, and communication platforms;

c. Implement user authentication, password management, multi-factor authentication, encryption, backup, disaster recovery, and access control measures;

d. Monitor organizational systems for cybersecurity threats, unauthorized access attempts, malware, ransomware, phishing, and other cyber risks;

e. Maintain audit logs and system activity records where appropriate;

f. Conduct vulnerability assessments and recommend remedial actions;

g. Ensure timely installation of security patches and software updates;

h. Support secure deployment of digital platforms, case management systems, and collaboration tools;

i. Advise Management on emerging technologies and associated privacy risks;

j. Participate in investigations relating to information security incidents;

k. Maintain secure backup and recovery procedures; and

l. Provide technical support for the implementation of this Policy.

The ICT Unit shall not access confidential information unless such access is necessary for legitimate technical administration, maintenance, incident response, or another authorized purpose.

2.24 Responsibilities of the Human Resources Unit

The Human Resources Unit shall ensure that privacy and confidentiality obligations are integrated into all employment-related processes.

The Unit shall:

a. Maintain secure personnel records;

b. Ensure confidential recruitment processes;

c. Incorporate confidentiality obligations into employment contracts;

d. Ensure all employees acknowledge this Policy during onboarding;

e. Coordinate mandatory data protection training;

f. Maintain disciplinary records securely;

g. Restrict access to personnel information on a need-to-know basis;

h. Ensure secure management of employee medical information, payroll records, leave records, and performance evaluations;

i. Coordinate exit procedures to recover organizational information assets; and

j. Ensure departing personnel continue to observe post-employment confidentiality obligations.

2.25 Responsibilities of the Legal Unit

The Legal Unit shall provide legal oversight concerning privacy, confidentiality, legal privilege, and information governance.

Its responsibilities include:

a. Advising Management on applicable legal obligations;

b. Reviewing data sharing agreements, memoranda of understanding, partnership agreements, and data processing agreements;

c. Advising on lawful disclosure of confidential information;

d. Protecting legal professional privilege;

e. Supporting investigations involving legal issues;

f. Monitoring legal developments affecting privacy and information governance;

g. Advising on litigation risks arising from data breaches; and

h. Assisting in the development and periodic review of this Policy.

2.26 Responsibilities of the MEAL Unit

The Monitoring, Evaluation, Accountability and Learning (MEAL) Unit shall ensure that all data collection, analysis, storage, reporting, and learning activities comply with this Policy.

The MEAL Unit shall:

a. Ensure that monitoring and evaluation activities collect only data that is necessary for approved programme purposes;

b. Develop data collection tools that incorporate privacy and confidentiality safeguards;

c. Ensure that beneficiary surveys, assessments, evaluations, complaints mechanisms, and accountability systems protect personal information;

d. Anonymize or pseudonymize data where individual identification is unnecessary;

e. Establish secure procedures for handling raw datasets, evaluation reports, and monitoring records;

f. Ensure that data used for reporting is accurate, complete, and appropriately protected;

g. Maintain secure storage of monitoring and evaluation records; and

h. Collaborate with programme teams to ensure responsible information management throughout the project cycle.

2.27 Responsibilities of Programme Departments

Programme Departments are responsible for ensuring that personal data collected during programme implementation is processed lawfully, fairly, securely, and in accordance with this Policy.

Programme Managers and Officers shall:

a. Collect only information necessary for programme delivery;

b. Ensure that beneficiaries are informed of the purpose for which their information is collected;

c. Maintain confidentiality of beneficiary records, legal aid files, safeguarding information, and community engagement documentation;

d. Protect information collected during field activities, outreach programmes, legal clinics, and community consultations;

e. Prevent unauthorized disclosure of beneficiary information;

f. Ensure secure transfer and storage of programme records; and

g. Promptly report any suspected or actual data breach affecting programme information.

2.28 Responsibilities of the Finance and Administration Department

The Finance and Administration Department shall ensure that financial, procurement, administrative, and operational information containing personal data is managed in accordance with this Policy and applicable financial management standards.

Without limiting its broader responsibilities, the Department shall:

a. Maintain secure financial records containing personal information;

b. Ensure confidentiality of payroll records, supplier information, banking details, tax records, reimbursement claims, and procurement documentation;

c. Implement appropriate controls over access to financial systems and accounting software;

d. Ensure that procurement records containing personal information are accessible only to authorized personnel;

e. Establish secure procedures for the transmission of payment instructions and financial documents;

f. Ensure compliance with donor confidentiality requirements relating to financial reporting;

g. Coordinate with the ICT Unit to secure electronic financial systems;

h. Maintain secure archival and disposal procedures for financial records; and

i. Promptly report any suspected or actual compromise of financial information.

2.29 Responsibilities of Project Managers and Team Leaders

Project Managers and Team Leaders shall be directly responsible for ensuring compliance with this Policy within their respective projects, programmes, or operational units.

They shall:

a. Ensure that project activities comply with the principles established under this Policy;

b. Supervise staff responsible for collecting or processing personal information;

c. Ensure that only authorized personnel access project information;

d. Monitor compliance during field activities;

e. Ensure secure storage of project records;

f. Verify that consultants, volunteers, and temporary personnel understand their confidentiality obligations;

g. Ensure that project reports appropriately anonymize personal information where individual identification is unnecessary;

h. Report privacy incidents without delay; and

i. Cooperate fully during audits, investigations, and compliance reviews.

2.30 Responsibilities of Employees

Every employee of ILA shares personal responsibility for protecting information entrusted to the Organization.

Every employee shall:

a. Comply fully with this Policy and all related procedures;

b. Process personal data only where authorized to do so;

c. Maintain strict confidentiality regarding all information acquired during employment;

d. Protect passwords, authentication credentials, and access devices;

e. Prevent unauthorized access to information;

f. Avoid discussing confidential matters in public places or with unauthorized persons;

g. Securely store paper and electronic records;

h. Immediately report suspected privacy incidents, cybersecurity events, or unauthorized disclosures;

i. Participate in mandatory training;

j. Cooperate during investigations and audits;

k. Exercise professional judgment when handling confidential information;

l. Protect organizational devices against theft, loss, or unauthorized use; and

m. Return all organizational information and information assets upon termination of employment.

Employees shall remain bound by confidentiality obligations after leaving the Organization.

2.31 Responsibilities of Volunteers and Interns

Volunteers and interns frequently access beneficiary information and organizational records while supporting programme implementation.

Accordingly, every volunteer and intern shall:

a. Sign a confidentiality undertaking before commencing duties;

b. Comply with this Policy;

c. Access information only as required for assigned responsibilities;

d. Refrain from copying, photographing, or removing confidential information without authorization;

e. Return all documents and devices upon completion of service;

f. Report suspected breaches immediately; and

g. Continue observing confidentiality obligations after completion of their engagement.

2.32 Responsibilities of Consultants and Contractors

Consultants and contractors engaged by ILA may process personal data while providing professional services.

Every consultancy agreement or service contract involving access to personal information shall include appropriate confidentiality and data protection provisions.

Consultants and contractors shall:

a. Process information only in accordance with written instructions issued by ILA;

b. Implement appropriate technical and organizational safeguards;

c. Maintain confidentiality throughout the engagement;

d. Prevent unauthorized disclosure;

e. Notify ILA immediately of any actual or suspected data breach;

f. Cooperate during investigations;

g. Return or securely destroy information upon completion of the assignment, as directed by ILA; and

h. Refrain from retaining copies of organizational information unless expressly authorized.

2.33 Responsibilities of Third-Party Data Processors

Third-party service providers, including cloud service providers, software vendors, payroll processors, external auditors, research institutions, hosting providers, consultants, and other entities processing personal information on behalf of ILA, shall comply with this Policy and any applicable contractual obligations.

Before engaging any third-party processor, ILA shall undertake appropriate due diligence to assess the provider's capacity to protect personal data.

Third-party processors shall:

a. Process personal data only for the purposes specified by ILA;

b. Implement appropriate technical and organizational security measures;

c. Maintain confidentiality;

d. Restrict access to authorized personnel;

e. Notify ILA promptly of any actual or suspected breach;

f. Permit reasonable audits where contractually required;

g. Refrain from engaging subcontractors without prior written approval from ILA;

h. Return or securely destroy information upon termination of the contractual relationship; and

i. Comply with applicable legal, contractual, and donor requirements.

2.34 Organizational Responsibility

Protection of personal information is a shared organizational responsibility.

No department may assume that responsibility rests exclusively with the ICT Unit, Human Resources Unit, Legal Unit, or any other specialized office.

Every department shall incorporate privacy and confidentiality considerations into:

- operational planning;
- programme implementation;
- procurement;

- recruitment;
- financial management;
- safeguarding;
- communications;
- research;
- monitoring and evaluation; and
- risk management.

Managers shall ensure that privacy considerations form part of routine supervisory responsibilities.

PART III

DATA PROTECTION COMMITTEE

2.35 Establishment

ILA shall establish a **Data Protection Committee (DPC)** as an internal advisory and oversight mechanism to strengthen organizational governance over personal data, information security, confidentiality, and privacy.

The Committee shall support Management in the implementation of this Policy and shall serve as a multidisciplinary forum for addressing significant data protection matters.

The Committee shall not replace the operational responsibilities assigned under this Policy but shall coordinate, advise, monitor, and recommend improvements to the Organization's data protection framework.

2.36 Composition

The Committee shall be appointed by the Executive Director and shall ordinarily comprise:

a. the Executive Director or a designated senior manager (Chairperson);

b. the Head of ICT or ICT Officer;

c. the Human Resources Manager or Officer;

d. the Finance and Administration Manager or Officer;

e. the Head of Programmes or designated Programme Manager;

f. the MEAL Manager or Officer;

g. the Legal Officer or Legal Adviser;

h. the Safeguarding Focal Person; and

i. any other officer co-opted by the Executive Director where specialized expertise is required.

The Committee may invite technical experts, consultants, or external advisers to attend meetings in an advisory capacity where necessary.

2.37 Functions of the Committee

The Data Protection Committee shall:

a. Monitor implementation of this Policy;

b. Review significant privacy and data protection risks;

c. Consider reports of major data breaches and recommend corrective actions;

d. Review findings from internal audits, compliance assessments, and external evaluations relating to data protection;

e. Advise Management on emerging legal, technological, operational, and cybersecurity developments;

f. Recommend improvements to organizational policies, procedures, and systems;

g. Oversee implementation of corrective action plans arising from data protection incidents;

h. Promote cross-departmental coordination on privacy matters;

i. Review Data Protection Impact Assessments for high-risk projects before implementation;

j. Support the development of organizational awareness and training programmes; and

k. Prepare an annual report on the state of data protection within ILA for submission to the Executive Director and, where appropriate, the Board of Directors.

2.38 Meetings

The Committee shall meet:

a. at least once every quarter;

b. following any major data breach or cybersecurity incident;

c. whenever requested by the Executive Director; or

d. where urgent privacy risks require immediate consideration.

Minutes of all meetings shall be maintained securely and treated as confidential organizational records.

PART IV

ACCOUNTABILITY FRAMEWORK

2.39 Individual Accountability

Every individual processing personal data on behalf of ILA remains personally accountable for ensuring that their actions comply with this Policy.

Delegation of authority does not remove personal responsibility for compliance.

Individuals shall be able to demonstrate that decisions relating to personal data were:

- lawful;
- reasonable;
- documented;
- proportionate;
- authorized; and
- consistent with this Policy.

Failure to comply may result in disciplinary, contractual, civil, or criminal consequences, as provided under Chapter Fourteen of this Policy and other applicable organizational instruments.

2.40 Organizational Accountability

ILA shall maintain documented evidence demonstrating its compliance with this Policy, including:

a. data inventories and records of processing activities;

b. access control logs;

c. confidentiality undertakings;

d. training attendance records;

e. incident and breach registers;

f. audit reports;

g. risk assessments;

h. Data Protection Impact Assessments;

i. corrective action plans;

j. records retention schedules; and

k. periodic compliance reviews.

The Organization shall periodically evaluate the effectiveness of its governance framework and implement improvements where deficiencies are identified.

PART V

PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

2.41 General Principle

ILA shall incorporate privacy and data protection considerations into the design, development, procurement, implementation, operation, maintenance, modification, and retirement of all programmes, projects, systems, technologies, policies, procedures, and operational activities that involve the processing of personal data.

Privacy shall not be treated as an afterthought or as a corrective measure implemented only after a risk has materialized. Instead, privacy considerations shall be integrated from the earliest stages of planning and shall continue throughout the entire information lifecycle.

Accordingly, every department shall consider the potential impact of proposed activities on the privacy rights of individuals before personal data is collected or processed.

2.42 Privacy by Design

Privacy by Design requires that privacy safeguards be proactively embedded into organizational processes and technologies rather than applied retrospectively.

In implementing this principle, ILA shall:

a. Identify privacy risks during the planning phase of new initiatives;

b. Integrate privacy considerations into project proposals, concept notes, programme designs, procurement processes, and system development;

c. Minimize the collection and use of personal data wherever feasible;

d. Implement technical safeguards that prevent unauthorized access, alteration, or disclosure of personal information;

e. Adopt secure system configurations as standard practice;

f. Incorporate confidentiality requirements into contracts, agreements, and terms of reference;

g. Ensure that privacy considerations are included in software selection, cloud services, and digital platforms;

h. Evaluate third-party technologies before deployment to ensure they provide appropriate privacy safeguards;

i. Document decisions affecting the processing of personal data; and

j. Periodically review systems and processes to verify that privacy controls remain effective.

2.43 Privacy by Default

ILA shall ensure that the default settings of its systems, applications, databases, forms, and operational procedures provide the highest level of privacy protection that is reasonably practicable.

Unless a documented operational need requires otherwise:

a. access to personal data shall be restricted to authorized personnel;

b. optional personal data fields shall not be mandatory;

c. information sharing shall be limited to those with a legitimate need to know;

d. user permissions shall be configured according to the principle of least privilege;

e. personal information shall not be publicly accessible;

f. automated retention periods shall not exceed organizational requirements; and

g. system logs shall record significant access to sensitive information where technically feasible.

Departments proposing any departure from these default protections shall document the justification and obtain appropriate management approval.

2.44 Privacy in Procurement and System Acquisition

Before acquiring or subscribing to any software, cloud service, digital platform, mobile application, artificial intelligence tool, or information management system, the responsible department shall, in consultation with the ICT Unit and the Legal Unit where appropriate, assess whether the proposed solution:

a. Incorporates appropriate privacy and security features;

b. Permits effective access control and authentication;

c. Supports encryption where required;

d. Provides audit logging capabilities;

e. Enables compliance with records retention requirements;

f. Allows secure deletion or export of organizational data;

g. Complies with applicable contractual and donor obligations; and

h. Presents any unacceptable privacy or cybersecurity risks.

No system shall be adopted where the identified risks outweigh the operational benefits and cannot be adequately mitigated.

PART VI

DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

2.45 Purpose

A Data Protection Impact Assessment (DPIA) is a structured process for identifying, assessing, documenting, and mitigating privacy risks before commencing processing activities that may significantly affect the rights, freedoms, or legitimate interests of individuals.

DPIAs support informed decision-making and ensure that privacy considerations are embedded into organizational planning and risk management.

2.46 Circumstances Requiring a DPIA

A DPIA shall be conducted before commencing any new activity that is likely to involve a high risk to individuals or to the Organization, including but not limited to:

a. Implementation of a new case management system;

b. Deployment of a beneficiary registration database;

c. Adoption of cloud-based information systems;

d. Introduction of biometric identification technologies;

e. Large-scale processing of sensitive personal data;

f. Processing of children's personal data on a significant scale;

g. Use of artificial intelligence or automated decision-making tools affecting individuals;

h. Integration of multiple databases containing personal information;

i. Large-scale monitoring, research, surveys, or evaluations involving identifiable individuals;

j. Cross-border transfers of sensitive personal data; or

k. Any other activity designated by the Executive Director or the Data Protection Committee as requiring enhanced assessment.

2.47 Contents of a DPIA

A DPIA shall, at a minimum:

a. Describe the proposed processing activity;

b. Identify the purpose and lawful basis for processing;

c. Identify the categories of personal data involved;

d. Identify affected individuals and stakeholder groups;

e. Assess the necessity and proportionality of the proposed processing;

f. Identify potential risks to privacy, confidentiality, and security;

g. Evaluate the likelihood and severity of identified risks;

h. Identify existing safeguards;

i. Recommend additional mitigation measures where necessary;

j. Identify residual risks after mitigation;

k. Assign implementation responsibilities; and

l. Document management approval before implementation.

Completed DPIAs shall be retained as confidential organizational records.

2.48 Review of DPIAs

Where significant changes occur to the nature, scope, purpose, technology, or risk profile of a processing activity, the relevant DPIA shall be reviewed and updated.

The Data Protection Committee may require periodic review of high-risk processing activities.

PART VII

INFORMATION GOVERNANCE RISK MANAGEMENT

2.49 Integration with Organizational Risk Management

Information governance and data protection risks shall form part of ILA's Enterprise Risk Management Framework.

Privacy risks shall be identified, analysed, evaluated, treated, monitored, and reported using the Organization's established risk management processes.

The Risk Management Committee and the Data Protection Committee shall coordinate where privacy risks intersect with broader organizational, operational, financial, legal, cybersecurity, or safeguarding risks.

2.50 Categories of Information Risk

For purposes of this Policy, information risks include, but are not limited to:

a. Unauthorized disclosure of confidential information;

b. Unauthorized access to information systems;

c. Cyberattacks;

d. Ransomware incidents;

e. Phishing and social engineering attacks;

f. Accidental disclosure of personal information;

g. Insider misuse of information;

h. Theft or loss of organizational devices;

i. Destruction or corruption of organizational records;

j. Inadequate records retention;

k. Improper disposal of records;

l. Unauthorized cross-border transfers;

m. Reputational harm arising from privacy failures; and

n. Non-compliance with legal, contractual, or donor obligations.

2.51 Information Risk Assessments

Departments processing personal information shall conduct periodic information risk assessments to identify vulnerabilities affecting the confidentiality, integrity, availability, and resilience of organizational information assets.

Risk assessments shall consider:

- the sensitivity of the information;
- the volume of data processed;
- the number of individuals affected;
- potential threats and vulnerabilities;
- existing safeguards;
- the likelihood of occurrence;
- the severity of potential harm; and
- proposed mitigation measures.

Risk assessments shall be documented and reviewed periodically or whenever significant operational changes occur.

PART VIII

REPORTING, MONITORING AND CONTINUOUS IMPROVEMENT

2.52 Internal Reporting

All personnel shall promptly report any suspected or actual:

a. Data breach;

b. Unauthorized disclosure;

c. Cybersecurity incident;

d. Attempted unauthorized access;

e. Loss or theft of records;

f. Loss or theft of organizational devices containing personal data;

g. System vulnerability;

h. Suspected misuse of confidential information; or

i. Any circumstance that could reasonably compromise the confidentiality, integrity, or availability of personal information.

Reports shall be made immediately to the staff member's supervisor and the ICT Unit, with notification to the Executive Director where the incident is significant.

No employee or volunteer shall suffer retaliation for making a report in good faith.

2.53 Monitoring and Assurance

ILA shall establish ongoing monitoring mechanisms to assess compliance with this Policy.

Monitoring activities may include:

a. Internal audits;

b. Compliance reviews;

c. Access log reviews;

d. Records management inspections;

e. Cybersecurity assessments;

f. Vulnerability assessments;

g. Penetration testing where appropriate;

h. Management reviews;

i. Donor compliance reviews; and

j. External independent assessments where necessary.

Findings shall be documented, reported to Management, and used to strengthen organizational controls.

2.54 Corrective and Preventive Actions

Where deficiencies are identified, Management shall ensure that appropriate corrective and preventive actions are implemented within reasonable timeframes.

Corrective actions may include:

- policy revisions;
- additional staff training;
- system enhancements;
- disciplinary measures;
- procurement of improved technologies;
- revision of operational procedures;
- enhanced supervision; and
- periodic follow-up assessments.

Implementation of corrective actions shall be monitored until completion.

2.55 Continuous Improvement

ILA is committed to continually strengthening its data protection and privacy management framework.

The Organization shall periodically review:

a. Technological developments;

b. Emerging cybersecurity threats;

c. Legal and regulatory developments;

d. Donor requirements;

e. Lessons learned from incidents;

f. Audit findings;

g. Staff feedback;

h. Beneficiary feedback; and

i. International best practices.

Where necessary, this Policy, related procedures, and operational controls shall be revised to ensure continued effectiveness and relevance.

CHAPTER THREE

CATEGORIES OF PERSONAL DATA AND DATA PROCESSING ACTIVITIES

3.1 Introduction

The Initiative for Legal Aid (ILA) processes a broad range of personal information in the course of implementing its programmes, delivering legal services, administering organizational operations, managing human resources, monitoring projects, engaging with donors, conducting research, safeguarding vulnerable persons, and fulfilling statutory and contractual obligations.

The nature of the Organization's work requires the processing of information that ranges from ordinary administrative records to highly sensitive legal, financial, medical, and safeguarding information. Improper handling of such information may expose individuals to physical harm, discrimination, retaliation, financial loss, psychological trauma, reputational damage, or other adverse consequences, while simultaneously exposing the Organization to legal, operational, financial, and reputational risks.

Accordingly, all personal data processed by ILA shall be identified, classified, processed, protected, retained, shared, archived, and disposed of in accordance with the provisions of this Policy.

The classification of information under this Chapter shall determine the level of security, confidentiality, access control, retention, disclosure, and oversight required throughout the information lifecycle.

PART I

PERSONAL DATA

3.2 Meaning of Personal Data

For the purposes of this Policy, **personal data** means any information relating to an identified or identifiable natural person.

A person is identifiable where they can be identified directly or indirectly by reference to one or more identifiers, whether alone or in combination with other information reasonably available to ILA.

Personal data may exist in paper, electronic, audio, visual, biometric, or any other form capable of identifying an individual.

3.3 Categories of Personal Data Processed by ILA

Without limitation, personal data processed by ILA may include:

A. Identification Information

Including:

- full names;
- former names;
- aliases where lawfully recorded;
- date of birth;
- place of birth;
- nationality;
- national identity number;
- passport number;
- refugee or asylum documentation;
- voter registration details;
- driver's licence information;
- employee identification numbers;
- staff identification cards;
- beneficiary registration numbers; and
- client reference numbers.

B. Contact Information

Including:

- residential addresses;
- postal addresses;
- telephone numbers;
- email addresses;
- emergency contacts;
- next of kin information;
- office addresses; and
- social media contact details where voluntarily provided.

C. Demographic Information

Including:

- age;
- gender;
- marital status;
- occupation;
- educational background;

- language preferences;
- disability information;
- household composition;
- geographical location;
- community affiliation; and
- socioeconomic indicators collected for programme purposes.

D. Employment Information

Including:

- curriculum vitae;
- academic qualifications;
- employment history;
- recruitment records;
- interview assessments;
- appointment letters;
- job descriptions;
- contracts of employment;
- performance evaluations;
- promotions;
- disciplinary records;
- attendance records;
- payroll information;
- pension information;
- tax information;
- leave records;
- training history;
- professional memberships; and
- exit interview records.

E. Financial Information

Including:

- bank account details;
- payment records;
- supplier payment information;
- reimbursement records;
- payroll records;
- taxation records;
- procurement information;
- grant disbursement information;
- financial declarations;
- conflict of interest declarations where financial interests are disclosed; and
- audit documentation containing personal information.

F. Digital Information

Including:

- usernames;
- login credentials (stored securely and never in plain text);
- IP addresses;
- device identifiers;
- browser information;
- audit logs;
- electronic signatures;
- system access records;
- metadata;
- cloud service activity records;
- mobile device identifiers; and
- digital communication records.

PART II

SPECIAL CATEGORIES OF PERSONAL DATA

3.4 General

Certain categories of personal data require enhanced protection because unauthorized disclosure may expose individuals to substantial harm or violate legal, ethical, or professional obligations.

ILA shall implement enhanced safeguards whenever processing special categories of personal data.

Access shall be limited strictly to authorized personnel with a demonstrable operational need.

3.5 Health Information

Health-related information may include:

- medical reports;
- disability information;
- psychological assessments;
- counselling records;
- occupational health records;
- medical certificates;
- injury reports;
- vaccination records where legitimately required;
- emergency medical information; and
- other information concerning an individual's physical or mental health.

Health information shall be treated as highly confidential.

Disclosure shall occur only where:

a. authorized by law;

b. required for safeguarding purposes;

c. necessary to protect life or prevent serious harm;

d. expressly authorized by the individual; or

e. otherwise permitted under this Policy.

3.6 Safeguarding Information

ILA frequently handles highly sensitive safeguarding information relating to:

- survivors of sexual exploitation or abuse;
- children;
- vulnerable adults;
- whistleblowers;
- complainants;
- witnesses;
- safeguarding investigations;
- referral pathways;
- psychosocial support;
- protection assessments; and
- case management documentation.

Safeguarding records shall receive the highest level of organizational protection.

Access shall be strictly limited to personnel directly involved in safeguarding responsibilities.

Safeguarding information shall never be disclosed except in accordance with safeguarding procedures, applicable law, court orders, or overriding protection considerations.

3.7 Children's Personal Data

Information relating to children requires enhanced protection because of children's particular vulnerability.

Where ILA processes children's personal data, the Organization shall:

a. Collect only information that is strictly necessary;

b. Consider the best interests of the child at all times;

c. Obtain consent from a parent, guardian, or other legally authorized representative where required, unless another lawful basis applies;

d. Implement enhanced confidentiality safeguards;

e. Avoid unnecessary publication or dissemination of identifying information;

f. Protect children's photographs, videos, and case records from unauthorized disclosure; and

g. Ensure that programme staff handling children's information receive appropriate safeguarding and confidentiality training.

3.8 Criminal Justice Information

ILA may process information concerning:

- arrests;
- detention;
- criminal investigations;
- prosecutions;
- convictions;
- rehabilitation;
- correctional records;
- witness protection;
- evidence; and
- court proceedings.

Such information shall be processed only where necessary for legal aid, litigation, human rights work, advocacy, research, or another legitimate organizational purpose.

PART III

LEGAL AID INFORMATION

3.9 Client Information

The confidentiality of legal aid client information is fundamental to the administration of justice and the relationship of trust between ILA and its clients.

Client information includes:

- legal advice;
- legal opinions;

- pleadings;
- affidavits;
- witness statements;
- litigation strategy;
- correspondence;
- evidence;
- settlement negotiations;
- mediation records;
- arbitration documents;
- court judgments;
- appeals;
- legal research;
- client interviews; and
- instructions received from clients.

Such information shall be protected by the highest standards of confidentiality and, where applicable, legal professional privilege.

3.10 Legal Professional Privilege

Nothing in this Policy shall be interpreted as limiting or diminishing the protection afforded by legal professional privilege.

Information protected by legal professional privilege shall not be disclosed except:

a. with informed client authorization;

b. pursuant to a lawful court order after consideration of applicable privileges;

c. where disclosure is required by law and privilege does not apply; or

d. in other exceptional circumstances recognized by applicable law.

ILA personnel engaged in legal practice shall observe all professional obligations concerning confidentiality and privilege.

3.11 Witness Information

Witness information frequently presents elevated security risks.

Accordingly, ILA shall implement enhanced safeguards for:

- witness identities;
- contact details;
- interview records;
- statements;

- testimony;
- protection measures;
- security assessments; and
- related documentation.

Disclosure of witness information shall be limited to those persons whose access is strictly necessary for legal proceedings, safeguarding, or security purposes.

PART IV

HUMAN RESOURCE INFORMATION

3.12 Personnel Records

The Human Resources Unit shall maintain secure personnel files for each employee, volunteer, intern, and consultant, containing only information necessary for employment, administration, legal compliance, and organizational management.

Personnel records may include:

- recruitment documentation;
- employment contracts;
- job descriptions;
- salary information;
- leave records;
- disciplinary records;
- grievances;
- training records;
- performance appraisals;
- declarations of interest;
- confidentiality undertakings;
- exit documentation; and
- other employment-related records.

Personnel records shall be maintained securely and shall only be accessed by authorized personnel.

3.13 Recruitment Information

Information collected during recruitment shall be processed solely for recruitment and employment purposes unless otherwise authorized by the applicant or required by law.

Applicants who are not appointed shall have their information retained only for the period specified in the Records Retention Schedule unless they consent to longer retention for future recruitment opportunities.

PART V

PROGRAMME, BENEFICIARY AND COMMUNITY INFORMATION

3.14 Beneficiary Information

ILA processes personal information relating to beneficiaries in the implementation of legal aid, access to justice, human rights, governance, civic education, legal empowerment, alternative dispute resolution, community outreach, and other programme activities.

Beneficiary information may include:

- beneficiary registration forms;
- names and contact information;
- demographic profiles;
- household composition;
- vulnerability assessments;
- socioeconomic information;
- legal needs assessments;
- programme eligibility information;
- attendance registers;
- service utilization records;
- referrals;
- follow-up records;
- beneficiary feedback;
- complaints;
- monitoring data; and
- programme exit assessments.

Such information shall be collected only to the extent necessary for legitimate programme purposes and shall be protected in accordance with this Policy.

3.15 Community Engagement Information

During community dialogues, consultations, legal awareness campaigns, public meetings, focus group discussions, stakeholder engagements, and outreach activities, ILA may collect personal information for programme implementation and accountability purposes.

Programme personnel shall ensure that:

a. participants are informed of the purpose for which information is collected;

b. participation is voluntary unless otherwise required by law or contractual obligations;

c. attendance registers are protected against unauthorized access;

d. photographs and recordings are obtained in accordance with this Policy;

e. reports avoid unnecessary disclosure of personal identifiers; and

f. community members are treated with dignity, respect, and confidentiality.

3.16 Complaints and Feedback Information

Information received through complaints handling mechanisms, feedback systems, whistleblowing channels, safeguarding reporting mechanisms, and accountability processes shall be treated as confidential.

Special protection shall be provided for information relating to:

- complainants;
- whistleblowers;
- survivors;
- witnesses;
- alleged perpetrators;
- investigators; and
- persons providing information in confidence.

Disclosure shall be strictly limited to individuals with an authorized role in receiving, assessing, investigating, or resolving the complaint.

PART VI

DONOR, PARTNER AND STAKEHOLDER INFORMATION

3.17 Donor Information

ILA shall protect confidential information received from donors, funding agencies, philanthropic organizations, foundations, and grant-making institutions.

Donor information may include:

- contact details;
- grant agreements;
- financial reports;
- due diligence documentation;
- audit reports;
- monitoring findings;
- confidential correspondence;
- payment information; and
- proprietary programme information.

Donor information shall be processed in accordance with contractual obligations and this Policy.

3.18 Partner Information

Information exchanged with implementing partners, consortium members, government institutions, civil society organizations, legal institutions, academic institutions, consultants, and service providers shall be protected against unauthorized disclosure.

Where information sharing arrangements exist, appropriate data-sharing agreements or confidentiality provisions shall govern such exchanges.

PART VII

RESEARCH, MONITORING, EVALUATION, ACCOUNTABILITY AND LEARNING (MEAL)

3.19 Research Information

Research undertaken by ILA shall respect the privacy, dignity, rights, and legitimate expectations of participants.

Researchers shall ensure that:

a. Only information necessary for the approved research objectives is collected;

b. Participants receive appropriate information regarding the research;

c. Informed consent is obtained where required;

d. Confidentiality is maintained;

e. Data is securely stored;

f. Identifiable information is minimized wherever practicable;

g. Publication does not unnecessarily identify participants; and

h. Research data is retained and disposed of in accordance with this Policy.

3.20 MEAL Information

The MEAL Unit processes substantial quantities of programme information for planning, monitoring, evaluation, accountability, learning, and reporting.

MEAL personnel shall ensure that:

a. Data collection tools collect only information necessary for programme objectives;

b. Beneficiary identifiers are minimized where possible;

c. Evaluation reports avoid unnecessary disclosure of personal information;

d. Raw datasets are securely stored;

e. Personal information is anonymized or pseudonymized before wider analysis wherever feasible;

f. Monitoring records are protected against unauthorized access; and

g. Donor reporting complies with confidentiality obligations.

PART VIII

DIGITAL INFORMATION AND ELECTRONIC COMMUNICATIONS

3.21 Electronic Communications

Emails, official messaging platforms, collaboration tools, video conferences, electronic correspondence, and other digital communications used for official business constitute organizational records where they relate to organizational activities.

Such communications shall be managed in accordance with this Policy and applicable records management requirements.

Personnel shall avoid transmitting sensitive personal information through unsecured channels.

3.22 Website Information

ILA's website may collect limited technical information necessary for website administration, security, analytics, and service improvement.

Such information may include:

- IP addresses;
- browser type;
- operating system;
- referring pages;
- device information;
- cookies;
- session information; and
- website usage statistics.

Where cookies or similar technologies are used, users shall be informed through an appropriate privacy notice.

3.23 Social Media Information

Official organizational social media platforms shall be administered responsibly.

Personnel managing official accounts shall ensure that:

a. confidential information is never published without authorization;

b. beneficiary identities are protected;

c. photographs are used only in accordance with consent requirements and safeguarding considerations;

d. comments containing personal information are appropriately managed; and

e. direct messages containing confidential information are handled securely.

PART IX

AUDIO, VISUAL AND BIOMETRIC INFORMATION

3.24 Photographs

Photographs may be collected for programme documentation, donor reporting, public awareness, advocacy, communications, fundraising, training, archival purposes, or other legitimate organizational activities.

Before photographing identifiable individuals, ILA shall, where appropriate:

a. Explain the intended purpose;

b. Obtain informed consent or other lawful authorization;

c. Consider safeguarding implications;

d. Avoid exposing vulnerable persons to unnecessary risk; and

e. Maintain secure storage of image files.

Additional safeguards shall apply where children or survivors are photographed.

3.25 Audio and Video Recordings

Audio and video recordings shall only be made where:

a. Necessary for legitimate organizational purposes;

b. Authorized by Management where required;

c. Participants have been appropriately informed, except where lawful investigative activities require otherwise; and

d. Appropriate safeguards are implemented.

Recordings shall not be retained longer than necessary.

3.26 CCTV

Where CCTV systems are deployed for security purposes, ILA shall:

a. Clearly identify monitored areas through appropriate signage;

b. Limit monitoring to legitimate security objectives;

c. Restrict access to recordings;

d. Retain recordings only for approved retention periods unless required for investigations or legal proceedings; and

e. Prohibit use of CCTV for unjustified surveillance of staff, beneficiaries, or visitors.

3.27 Biometric Information

Biometric information, including fingerprints, facial recognition data, iris scans, voiceprints, or other biometric identifiers, shall only be collected where:

a. There is a lawful basis;

b. The purpose cannot reasonably be achieved through less intrusive means;

c. Appropriate security safeguards are implemented;

d. Management has approved the processing; and

e. The rights and legitimate interests of affected individuals are adequately protected.

Biometric data shall be classified as **Highly Confidential Information**.

PART X

ANONYMIZATION, PSEUDONYMIZATION AND AGGREGATION

3.28 Anonymized Data

Information that has been irreversibly anonymized so that individuals can no longer be identified is not regarded as personal data for the purposes of this Policy.

Departments are encouraged to use anonymized information wherever operationally feasible.

3.29 Pseudonymized Data

Where complete anonymization is impracticable, departments shall consider pseudonymization techniques, including:

- coded identifiers;
- reference numbers;
- encrypted identifiers; and
- separate storage of identifying information.

The key linking pseudonyms to identifiable individuals shall be protected separately with enhanced security controls.

3.30 Aggregated Data

Aggregated information prepared for statistical analysis, programme reporting, research, advocacy, donor reporting, or public communications should avoid identifying individual persons unless identification is expressly authorized or required.

PART XI

DATA CLASSIFICATION FRAMEWORK

3.31 Purpose

ILA adopts a formal Data Classification Framework to ensure that information is protected according to its sensitivity, value, legal obligations, and potential impact if disclosed, altered, or lost.

Every document, dataset, database, electronic file, communication, and information asset shall be assigned an appropriate classification.

3.32 Classification Levels

ILA shall classify information into the following categories:

A. Public Information

Information approved for unrestricted public release, including:

- published reports;
- approved press releases;
- publicly available policy documents;
- recruitment advertisements;
- publications;
- newsletters; and
- approved website content.

Public information may be disclosed without restriction, subject to organizational approval processes.

B. Internal Information

Information intended for internal organizational use that would not ordinarily cause significant harm if disclosed but is not intended for public distribution.

Examples include:

- internal meeting agendas;
- operational procedures;
- staff directories;
- routine administrative communications; and
- draft working documents.

C. Confidential Information

Information whose unauthorized disclosure could adversely affect individuals, organizational operations, contractual relationships, or legal obligations.

Examples include:

- personnel records;
- financial information;
- procurement evaluations;
- donor correspondence;
- internal audit reports;
- legal advice; and
- programme records containing personal information.

Access shall be limited to authorized personnel on a need-to-know basis.

D. Highly Confidential Information

Information requiring the highest level of protection due to the severe consequences that could result from unauthorized disclosure.

This includes:

- legal aid case files;
- information protected by legal professional privilege;
- safeguarding case files;
- PSEA investigations;
- child protection records;
- whistleblower identities;
- witness protection information;
- medical records;
- biometric data;
- passwords and cryptographic keys;
- cybersecurity incident investigations; and
- information designated by the Executive Director or the Data Protection Committee as Highly Confidential.

Such information shall be subject to enhanced technical, administrative, and physical safeguards.

3.33 Classification Responsibilities

Every employee creating, receiving, or maintaining information shall ensure that the information is appropriately classified.

Where uncertainty exists regarding the appropriate classification, the matter shall be referred to the employee's supervisor, the ICT Unit, or the Legal Unit for guidance.

Managers shall periodically review information holdings within their departments to ensure that classifications remain appropriate.

CHAPTER FOUR

LAWFUL BASES FOR PROCESSING PERSONAL DATA

4.1 Purpose

The Initiative for Legal Aid (ILA) shall process personal data only where there exists a lawful, legitimate, and documented basis for doing so. Every activity involving the collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, transfer, restriction, retention, archiving, or destruction of personal data shall be capable of justification under one or more lawful bases recognized by this Policy and applicable law.

The identification of a lawful basis is a mandatory requirement before personal data is processed. Departments shall document the lawful basis relied upon for significant or high-risk processing activities and shall review that basis whenever the purpose or nature of the processing changes.

The mere availability of personal data does not authorize its collection or use. Information that is publicly accessible, shared informally, or obtained from third parties shall not be processed unless a lawful basis exists.

PART I

GENERAL PRINCIPLES

4.2 Requirement for a Lawful Basis

Before collecting or processing personal data, the responsible department shall:

a. Identify the purpose of the processing;

b. Determine the applicable lawful basis;

c. Assess whether the processing is necessary and proportionate to the intended purpose;

d. Determine whether any special safeguards apply, particularly for sensitive personal data;

e. Document the lawful basis where required; and

f. Ensure that affected individuals are informed of the processing through an appropriate privacy notice, unless an exception recognized by law or this Policy applies.

Where multiple lawful bases apply to a single processing activity, ILA may rely on more than one basis, provided each is documented and applied consistently.

4.3 Necessity and Proportionality

Processing shall be limited to what is reasonably necessary to achieve the identified purpose. Departments shall avoid excessive, speculative, or unrelated collection of personal data.

In determining necessity and proportionality, ILA shall consider:

- whether the objective can be achieved with less personal data;
- whether anonymized or pseudonymized data would suffice;
- the sensitivity of the information;
- the potential impact on individuals;
- available safeguards; and
- the balance between organizational objectives and individual rights.

PART II

CONSENT

4.4 Processing Based on Consent

Where consent is relied upon as the lawful basis for processing, it shall be:

a. Freely given;

b. Specific to the intended purpose;

c. Informed;

d. Unambiguous; and

e. Capable of being demonstrated through appropriate records.

Consent shall not be obtained through coercion, deception, undue influence, or by making the provision of unnecessary personal data a condition for receiving services where such information is not required.

4.5 Obtaining Consent

Consent may be obtained in writing, electronically, verbally (where appropriately documented), or by another clear affirmative action appropriate to the circumstances.

The request for consent shall be presented in plain, understandable language and shall explain:

a. the identity of ILA;

b. the purpose of processing;

c. the categories of personal data to be collected;

d. any intended disclosures to third parties;

e. the anticipated retention period, where practicable;

f. the individual's rights under this Policy; and

g. the procedure for withdrawing consent.

Where literacy, language, disability, or vulnerability may affect understanding, ILA shall take reasonable measures to ensure that consent is genuinely informed.

4.6 Withdrawal of Consent

Individuals who have provided consent may withdraw that consent at any time, subject to legal, contractual, or operational limitations.

Withdrawal of consent shall not affect the lawfulness of processing undertaken before the withdrawal.

Upon receiving a valid withdrawal request, the responsible department shall:

a. assess whether another lawful basis permits continued processing;

b. cease processing where no alternative lawful basis exists;

c. update organizational records; and

d. inform the individual of the outcome within a reasonable period.

4.7 Situations Where Consent Is Not Required

Consent shall not be required where processing is lawfully undertaken on another recognized basis, including:

a. compliance with a legal obligation;

b. performance of a contract;

c. protection of vital interests;

d. legitimate organizational interests that are not overridden by the rights of the individual;

e. legal proceedings or legal advice;

f. safeguarding obligations;

g. humanitarian protection activities; or

h. another lawful basis recognized under this Policy or applicable law.

ILA shall not rely on consent where another lawful basis more accurately reflects the nature of the processing.

PART III

PERFORMANCE OF A CONTRACT

4.8 Contractual Necessity

Personal data may be processed where such processing is necessary for the performance of a contract to which the individual is a party or to take steps at the request of the individual prior to entering into a contract.

Examples include:

- employment contracts;
- consultancy agreements;
- internship agreements;
- volunteer agreements;
- supplier contracts;
- service agreements;
- grant agreements;
- lease agreements; and
- other lawful contractual arrangements.

Processing under this lawful basis shall be limited to what is necessary for the administration, performance, enforcement, or termination of the relevant contract.

PART IV

COMPLIANCE WITH LEGAL OBLIGATIONS

4.9 Legal Obligations

ILA may process personal data where necessary to comply with legal or regulatory obligations imposed under the laws of the Republic of South Sudan or other applicable legal requirements.

Such obligations may include:

a. Employment and labour requirements;

b. Taxation and financial reporting;

c. Audit obligations;

d. Court orders;

e. Lawful requests from competent authorities;

f. Statutory reporting requirements;

g. Anti-money laundering and counter-fraud obligations;

h. Occupational health and safety requirements; and

i. Record-keeping obligations.

Departments shall ensure that disclosures made pursuant to legal obligations are limited to the information required and are appropriately documented.

PART V

PROTECTION OF VITAL INTERESTS

4.10 Vital Interests

Personal data may be processed where necessary to protect the life, health, safety, or other vital interests of an individual or another person.

This lawful basis shall generally be relied upon only where the individual is incapable of giving consent or where immediate action is required.

Examples include:

- medical emergencies;
- evacuation during security incidents;
- locating family members during humanitarian emergencies;
- safeguarding children or vulnerable adults from imminent harm; and
- responding to life-threatening situations affecting staff, beneficiaries, or visitors.

Processing under this basis shall cease once the emergency has ended unless another lawful basis applies.

PART VI

LEGITIMATE ORGANIZATIONAL INTERESTS

4.11 Legitimate Interests

ILA may process personal data where such processing is necessary to pursue legitimate organizational interests, provided those interests are not overridden by the rights, freedoms, or legitimate expectations of the individual.

Legitimate interests may include:

a. programme planning and administration;

b. organizational governance;

c. information security;

d. fraud prevention and investigation;

e. internal auditing;

f. organizational risk management;

g. business continuity planning;

h. protection of organizational assets;

i. quality assurance;

j. statistical analysis using appropriate safeguards; and

k. responding to complaints, disputes, or legal claims.

Before relying on this basis, the responsible department shall conduct a documented assessment to ensure that the legitimate interest pursued is necessary, proportionate, and balanced against the potential impact on the individual.

4.12 Legitimate Interest Assessment (LIA)

Where legitimate interests are relied upon, an LIA should ordinarily consider:

a. the purpose of the processing;

b. the necessity of the processing;

c. whether a less intrusive alternative exists;

d. the reasonable expectations of affected individuals;

e. the risks to individual rights and freedoms;

f. safeguards to mitigate identified risks; and

g. whether the legitimate interests of ILA outweigh any adverse impact on the individual.

The LIA shall be documented for processing activities involving significant volumes of personal data or elevated privacy risks.

PART VII

PROCESSING IN THE PUBLIC INTEREST AND HUMANITARIAN ACTIVITIES

4.13 Public Interest Processing

ILA may process personal data where such processing is necessary for activities undertaken in the public interest and is consistent with the Organization's charitable mandate, legal obligations, and applicable law.

Public interest processing may include:

a. promotion of access to justice;

b. legal empowerment programmes;

c. public legal education;

d. human rights monitoring and documentation;

e. rule of law initiatives;

f. civic engagement and governance programmes;

g. strategic litigation supporting constitutional or public interest objectives;

h. policy research and legal reform initiatives; and

i. collaboration with competent public institutions where such collaboration serves a legitimate public interest.

Processing under this basis shall be limited to what is necessary to achieve the identified public interest objective and shall be subject to appropriate safeguards to protect individual rights.

4.14 Humanitarian and Emergency Response

Where ILA is involved in humanitarian response, emergency legal assistance, displacement response, disaster recovery, conflict-related interventions, or protection activities, personal data may be processed where necessary to:

a. identify persons requiring assistance;

b. facilitate referrals to competent service providers;

c. coordinate humanitarian interventions;

d. protect individuals from imminent harm;

e. reunite family members where appropriate;

f. document urgent protection concerns; or

g. comply with humanitarian coordination requirements.

Even in emergencies, only the minimum personal data necessary for the response shall be collected and processed.

PART VIII

LEGAL PROCEEDINGS, LEGAL ADVICE, AND DISPUTE RESOLUTION

4.15 Processing for Legal Services

As a legal aid organization, ILA may process personal data where necessary for the provision of legal advice, legal representation, mediation, arbitration, negotiation, legal counselling, strategic litigation, public interest litigation, or other lawful legal services.

Processing may include:

a. client intake and registration;

b. conflict-of-interest checks;

c. legal research;

d. preparation of pleadings and court documents;

e. communication with clients, courts, opposing parties, and relevant authorities;

f. evidence gathering and review;

g. witness interviews and statements;

h. legal analysis and opinion writing;

i. settlement negotiations;

j. enforcement of judgments; and

k. post-judgment follow-up.

Such processing shall be undertaken in accordance with applicable legal and ethical obligations, including legal professional privilege where applicable.

4.16 Litigation and Dispute Resolution

Personal data may also be processed where necessary to:

a. establish, exercise, or defend legal rights;

b. investigate legal claims;

c. respond to legal proceedings;

d. comply with court procedures;

e. participate in mediation or arbitration;

f. preserve evidence; or

g. enforce contractual or statutory rights.

Access to litigation files shall be restricted to authorized personnel directly involved in the matter.

PART IX

RESEARCH, STATISTICS, AND LEARNING

4.17 Research Processing

ILA may process personal data for research, monitoring, evaluation, accountability, learning, policy development, or statistical purposes, provided that:

a. the processing serves a legitimate organizational objective;

b. identifiable data is minimized wherever practicable;

c. participants are appropriately informed where required;

d. confidentiality is maintained;

e. published outputs do not unnecessarily identify individuals; and

f. appropriate safeguards are implemented throughout the research lifecycle.

Where feasible, anonymized or pseudonymized information shall be used in place of directly identifiable personal data.

4.18 Statistical and Analytical Processing

Personal data may be processed to produce aggregated statistics, trend analyses, performance indicators, programme evaluations, donor reports, and institutional learning products.

Reports intended for public dissemination should use aggregated or anonymized information unless there is a lawful basis for identifying individuals.

PART X

SAFEGUARDING AND PROTECTION ACTIVITIES

4.19 Processing for Safeguarding Purposes

ILA may process personal data where necessary to prevent, detect, investigate, or respond to safeguarding concerns involving children, vulnerable adults, beneficiaries, staff members, volunteers, or other persons associated with the Organization.

Processing may include:

a. receipt of safeguarding complaints;

b. risk assessments;

c. referral to appropriate protection services;

d. investigation of safeguarding allegations;

e. implementation of protective measures;

f. case management;

g. reporting to competent authorities where required by law; and

h. monitoring compliance with safeguarding obligations.

Safeguarding information shall be handled with the highest degree of confidentiality and shared only with persons who have a legitimate operational need or a lawful authority to receive it.

4.20 Child Protection

Where personal data relating to children is processed, ILA shall ensure that:

a. the best interests of the child are a primary consideration;

b. information collected is limited to what is necessary;

c. enhanced confidentiality safeguards are applied;

d. publication of identifying information is avoided unless clearly justified and lawfully authorized;

e. access is restricted to appropriately authorized personnel; and

f. all processing complies with the Organization's Child Protection and Safeguarding policies.

PART XI

PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

4.21 General Rule

Special categories of personal data shall be processed only where:

a. the processing is strictly necessary for a lawful purpose;

b. appropriate technical and organizational safeguards are implemented;

c. access is limited to authorized personnel;

d. the information is handled with enhanced confidentiality; and

e. at least one lawful basis recognized under this Policy applies.

Departments shall document the justification for processing sensitive personal data, particularly where large volumes of such information are involved.

4.22 Additional Safeguards

Processing of sensitive personal data shall, where appropriate, include:

a. encryption during storage and transmission;

b. enhanced authentication controls;

c. role-based access restrictions;

d. secure physical storage for paper records;

e. confidentiality undertakings by authorized personnel;

f. detailed access logging where technically feasible;

g. periodic review of access rights; and

h. secure destruction following the applicable retention period.

PART XII

DOCUMENTATION OF PROCESSING ACTIVITIES

4.23 Records of Processing

ILA shall maintain appropriate documentation demonstrating the lawful basis for significant processing activities.

Such records may include:

a. the purpose of processing;

b. the lawful basis relied upon;

c. categories of personal data processed;

d. categories of data subjects;

e. recipients of personal data;

f. applicable retention periods;

g. security measures implemented;

h. identified risks and mitigation measures;

i. Data Protection Impact Assessments, where applicable; and

j. any relevant approvals or authorizations.

These records shall support accountability, internal oversight, donor compliance, and audit requirements.

4.24 Change of Purpose

Where ILA intends to process personal data for a purpose materially different from the original purpose for which it was collected, the responsible department shall:

a. Assess whether the new purpose is compatible with the original purpose;

b. Determine whether the existing lawful basis remains applicable;

c. Identify whether additional consent or another lawful basis is required;

d. Update relevant documentation; and

e. Provide additional notice to affected individuals where appropriate.

If the new purpose is incompatible with the original purpose and no lawful basis exists, the processing shall not proceed.

PART XIII

PROHIBITED PROCESSING ACTIVITIES

4.25 Prohibited Processing

Unless expressly authorized by applicable law, this Policy, or a valid contractual obligation, ILA personnel shall not:

a. Collect personal data for speculative or undefined purposes;

b. Process personal data for personal gain or private interests;

c. Access information without authorization or a legitimate operational need;

d. Disclose confidential information to unauthorized persons;

e. Sell, trade, lease, or otherwise commercialize personal data;

f. Use personal data for discriminatory, retaliatory, or unlawful purposes;

g. Create unofficial databases containing organizational personal data;

h. Remove confidential records from organizational custody without authorization;

i. Circumvent established security controls;

j. Retain personal data beyond the approved retention period without lawful justification;

k. Use personal devices or unapproved applications to store highly confidential information unless expressly authorized and protected by approved security controls; or

l. Knowingly process personal data in a manner that violates this Policy or applicable law.

Any suspected breach of these prohibitions shall be reported immediately and managed in accordance with the Data Breach Management and Disciplinary provisions of this Policy.

CHAPTER FIVE

COLLECTION OF PERSONAL DATA

5.1 Introduction

The collection of personal data is the foundation upon which all subsequent processing activities depend. Information collected improperly, excessively, unlawfully, or without adequate safeguards may create significant risks to individuals and expose ILA to legal, operational, ethical, and reputational consequences.

The Initiative for Legal Aid (ILA) shall ensure that all personal data is collected in a manner that is lawful, fair, transparent, proportionate, secure, and consistent with the principles established under this Policy.

All departments, employees, volunteers, consultants, and third parties acting on behalf of ILA shall comply with the requirements of this Chapter whenever collecting information relating to identifiable individuals.

PART I

GENERAL REQUIREMENTS FOR DATA COLLECTION

5.2 Lawful and Fair Collection

ILA shall collect personal data only where:

a. A lawful basis for processing has been identified;

b. The collection serves a legitimate organizational purpose;

c. The information collected is necessary and proportionate;

d. Individuals are treated fairly and respectfully; and

e. Appropriate safeguards are applied during collection.

Personal data shall not be collected through deception, intimidation, coercion, unnecessary intrusion, or other unfair practices.

5.3 Collection for Specific Purposes

Before collecting personal data, the responsible department shall identify and document:

a. The purpose for collection;

b. The intended use of the information;

c. The persons or departments who may access the information;

d. Whether the information may be shared with third parties;

e. The applicable retention period; and

f. The safeguards required for protection.

Information shall not be collected merely because it may be useful in the future.

5.4 Data Minimization at Collection

ILA shall collect only the minimum amount of personal data necessary to achieve the identified purpose.

Collection forms, questionnaires, registration documents, interview templates, legal intake forms, employment forms, and electronic databases shall be reviewed periodically to ensure that unnecessary information is removed.

Examples of excessive collection may include:

- requesting personal information unrelated to programme eligibility;
- collecting unnecessary copies of identity documents;
- recording sensitive information without justification; or
- requiring disclosure of private information where less intrusive alternatives exist.

5.5 Accuracy at the Point of Collection

Reasonable measures shall be taken to ensure that information collected by ILA is accurate, complete, and reliable.

Personnel collecting information shall:

a. Verify critical information where appropriate;

b. Provide individuals an opportunity to correct inaccurate information;

c. Avoid assumptions when recording personal details;

d. Distinguish between confirmed facts and unverified information; and

e. Accurately record the source of information where relevant.

PART II

INFORMATION PROVIDED TO INDIVIDUALS AT COLLECTION

5.6 Privacy Information Notice

At the time personal data is collected, ILA shall provide individuals with appropriate information explaining how their data will be processed.

The privacy notice shall ordinarily include:

a. The identity of ILA;

b. The purpose of collecting the information;

c. The categories of information being collected;

d. The lawful basis for processing;

e. How the information will be used;

f. Who may receive or access the information;

g. Applicable retention periods;

h. Security measures applied;

i. Individual rights under this Policy;

j. Procedures for complaints or inquiries; and

k. Contact details for responsible organizational officers.

5.7 Accessible Privacy Notices

Privacy information shall be communicated in a manner appropriate to the individual concerned.

ILA shall consider:

- literacy levels;
- language preferences;
- disability;
- age;
- cultural context;
- vulnerability; and
- the urgency of the situation.

Where appropriate, privacy information may be provided through:

- written notices;
- translated materials;
- verbal explanations;
- audio formats;
- accessible digital formats; or
- other suitable communication methods.

PART III

DIRECT COLLECTION FROM INDIVIDUALS

5.8 General Rule

Where reasonably practicable, ILA shall collect personal data directly from the individual concerned.

Direct collection supports transparency, accuracy, informed participation, and accountability.

Direct collection may occur through:

a. Legal aid intake interviews;

b. Beneficiary registration;

c. Employment applications;

d. Contracts and agreements;

c. Surveys and questionnaires;

d. Monitoring visits;

e. Complaints mechanisms;

f. Interviews;

g. Consultations;

h. Training registration;

i. Procurement processes; and

j. Electronic platforms.

5.9 Interviews and Client Consultations

Given ILA's legal aid mandate, personal information is frequently obtained through interviews, consultations, and confidential discussions.

Personnel conducting interviews shall:

a. Explain their role and purpose;

b. Explain confidentiality limitations where applicable;

c. Collect only relevant information;

d. Ensure privacy during discussions;

e. Avoid unnecessary recording of sensitive details;

f. Accurately document information provided;

g. Protect interview notes and recordings;

h. Obtain authorization before making recordings; and

i. Immediately secure documents after completion.

5.10 Legal Aid Intake Information

Legal aid intake procedures shall collect sufficient information to:

- assess eligibility;
- identify legal issues;
- conduct conflict checks;
- provide appropriate assistance;
- manage legal proceedings; and
- comply with professional obligations.

However, intake processes shall avoid collecting unrelated personal information.

Client files shall be classified as **Highly Confidential Information** unless otherwise determined.

PART IV

COLLECTION FROM CHILDREN AND VULNERABLE PERSONS

5.11 Enhanced Protection Requirement

When collecting personal data from children, survivors of violence, displaced persons, persons with disabilities, vulnerable adults, witnesses, or other at-risk individuals, ILA shall apply enhanced safeguards.

Personnel shall consider:

a. Whether collection is necessary;

b. Whether the individual understands the purpose of collection;

c. Whether consent or authorization is required;

d. Whether collection may expose the individual to harm;

e. Whether additional confidentiality measures are necessary; and

f. Whether referral or safeguarding procedures are required.

5.12 Child Data Collection

When collecting information relating to children, ILA shall:

a. Prioritize the best interests of the child;

b. Avoid collecting unnecessary identifying information;

c. Obtain appropriate consent or authorization where required;

d. Explain information use in child-appropriate language where appropriate;

e. Protect children's images and personal stories;

f. Restrict access to authorized personnel; and

g. Ensure compliance with safeguarding procedures.

5.13 Vulnerable Individuals

Special consideration shall be given when collecting information from individuals who may face increased risks due to:

- conflict situations;
- displacement;
- disability;
- poverty;
- social exclusion;
- legal vulnerability;
- threats or intimidation;
- previous trauma; or
- dependence on assistance.

Collection practices shall avoid causing further harm or exposing individuals to unnecessary risks.

PART V

COLLECTION FROM THIRD PARTIES

5.14 Indirect Collection

ILA may obtain personal data from third-party sources where lawful and necessary for legitimate organizational purposes.

Third-party sources may include:

- courts;
- government institutions;
- referral organizations;
- partner organizations;
- donors;
- service providers;
- community structures;

- family representatives;
- legal representatives;
- publicly available records; and
- research sources.

5.15 Requirements for Third-Party Collection

Before collecting information from third parties, ILA shall assess:

a. Whether the source is authorized to provide the information;

b. Whether the collection is necessary;

c. Whether the information is accurate and reliable;

d. Whether the individual should be informed;

e. Whether confidentiality restrictions apply; and

f. Whether a data-sharing agreement is required.

5.16 Information Received from Courts and Authorities

Where ILA receives personal information from courts, government institutions, law enforcement agencies, or other competent authorities, such information shall be handled according to:

- applicable legal requirements;
- confidentiality obligations;
- court restrictions;
- professional duties; and
- this Policy.

PART VI

FIELD DATA COLLECTION

5.17 Field Operations

During field activities, including legal clinics, community outreach, monitoring visits, investigations, and assessments, personnel shall ensure that personal information is collected securely.

Field personnel shall:

a. Use approved collection tools;

b. Protect paper records from unauthorized viewing;

c. Avoid discussing personal matters publicly;

d. Secure electronic devices;

e. Avoid storing sensitive information on personal devices without authorization;

f. Transfer collected information securely; and

g. Report any loss, theft, or unauthorized disclosure immediately.

5.18 Mobile Data Collection

Where digital tools are used for field data collection, ILA shall ensure:

a. Authorized user accounts;

b. Password protection;

c. Secure transmission;

d. Appropriate encryption where available;

e. Controlled access;

f. Regular synchronization and backup procedures; and

g. Deletion of unnecessary local copies.

PART VII

ELECTRONIC AND ONLINE DATA COLLECTION

5.19 Digital Collection Platforms

Where ILA collects personal data through electronic systems, websites, mobile applications, online forms, databases, digital registration platforms, or other technology-enabled tools, such collection shall comply with this Policy and applicable information security requirements.

Before deploying any digital collection platform, the responsible department shall ensure that:

a. The purpose of collection is clearly defined;

b. Only necessary information fields are included;

c. Appropriate privacy notices are provided;

d. Access controls are implemented;

e. Information transmission is secure;

f. Unauthorized access risks are assessed;

g. Data retention requirements are established; and

h. The system has been reviewed by the ICT Unit where necessary.

5.20 Online Forms and Electronic Questionnaires

Electronic forms used for registration, surveys, feedback collection, recruitment, training, research, or programme monitoring shall:

a. Clearly identify ILA as the collecting organization;

b. Explain the purpose of collection;

c. Identify mandatory and optional information fields;

d. Avoid collecting unnecessary sensitive information;

e. Incorporate appropriate consent mechanisms where required;

f. Restrict access to authorized personnel; and

g. Maintain appropriate audit records where technically possible.

5.21 Cookies and Website Technologies

Where ILA websites or online platforms use cookies, tracking technologies, analytics tools, or similar technologies, the Organization shall ensure that:

a. users are informed of such technologies;

b. only necessary technical information is collected by default;

c. unnecessary tracking is avoided;

d. third-party tools are assessed before use; and

e. collected information is protected against misuse.

PART VIII

CONSENT COLLECTION PROCEDURES

5.22 General Requirements for Consent

Where consent is required as the lawful basis for collection, ILA shall ensure that consent is:

a. voluntary;

b. informed;

c. specific;

d. understandable;

e. documented; and

f. capable of withdrawal.

Consent shall not be assumed merely because an individual provides information.

5.23 Written Consent

Written consent may be obtained through:

- signed consent forms;
- signed declarations;
- employment documents;
- programme participation forms;
- research participation forms;
- electronic signatures; or
- other approved documentation methods.

Consent records shall be retained securely.

5.24 Verbal Consent

Where written consent is impractical, verbal consent may be obtained where appropriate, provided that:

a. the individual has been adequately informed;

b. the circumstances justify verbal consent;

c. the person obtaining consent records the consent;

d. the date, purpose, and nature of consent are documented; and

e. confidentiality safeguards remain applicable.

5.25 Consent for Images and Public Communications

Separate consent shall ordinarily be obtained before using identifiable photographs, videos, personal stories, testimonials, or case studies for:

- public advocacy;
- fundraising;
- publications;
- social media;
- websites;
- donor communications; or
- promotional materials.

Such consent shall explain:

a. where the material may appear;

b. the intended audience;

c. whether publication may involve public access;

d. the individual's right to refuse; and

e. any limitations on withdrawal after publication.

PART IX

COLLECTION OF PHOTOGRAPHS, AUDIO AND VIDEO RECORDINGS

5.26 General Requirements

Photographs, audio recordings, and video recordings may contain personal information and shall be collected responsibly.

Before collecting such information, ILA shall consider:

a. whether collection is necessary;

b. whether less intrusive alternatives exist;

c. whether individuals understand the purpose;

d. whether consent is required;

e. whether the collection creates security risks; and

f. how the information will be stored and used.

5.27 Images of Children and Vulnerable Persons

Images involving children, survivors of abuse, witnesses, displaced persons, or other vulnerable individuals require enhanced safeguards.

ILA shall:

a. avoid identifying vulnerable persons unnecessarily;

b. avoid revealing locations or circumstances that create risks;

c. obtain appropriate authorization;

d. avoid portraying individuals in a manner that undermines dignity;

e. securely store images; and

f. restrict publication unless clearly justified and approved.

PART X

COLLECTION FOR RESEARCH AND MEAL ACTIVITIES

5.28 Ethical Data Collection

Research and MEAL activities shall comply with ethical standards governing information collection.

Before collecting information for research or evaluation purposes, responsible personnel shall ensure:

a. the purpose is clearly defined;

b. participants understand their involvement;

c. participation is voluntary where appropriate;

d. confidentiality safeguards are explained;

e. unnecessary identifiers are avoided;

f. collected information is securely managed; and

g. findings are presented responsibly.

5.29 Surveys and Assessments

Survey instruments, questionnaires, and assessment tools shall be reviewed to ensure:

a. questions are relevant to the objective;

b. sensitive questions are justified;

c. participants understand why information is requested;

d. responses are protected;

e. data quality is maintained; and

f. findings do not expose individuals to harm.

PART XI

COLLECTION THROUGH HUMAN RESOURCES PROCESSES

5.30 Recruitment Data Collection

During recruitment, ILA may collect information necessary to assess suitability for employment or engagement.

Such information may include:

- identification details;
- qualifications;
- employment history;
- references;
- professional credentials;
- background information where lawfully required; and
- interview assessments.

Recruitment information shall not be used for unrelated purposes without a lawful basis.

5.31 Employee Records Collection

Upon engagement, ILA may collect additional information necessary for:

- employment administration;
- payroll;
- taxation;
- benefits;
- performance management;
- training;
- workplace safety;
- compliance obligations; and
- organizational planning.

The collection of employee information shall comply with the Human Resource Manual and this Policy.

PART XII

COLLECTION THROUGH COMPLAINTS AND INVESTIGATIONS

5.32 Complaints Information

Information received through complaint mechanisms shall be collected and managed in a manner that protects:

- complainants;
- respondents;
- witnesses;

- investigators;
- affected communities; and
- other persons involved.

Complaints procedures shall ensure confidentiality, impartiality, fairness, and protection against retaliation.

5.33 Investigation Information

During internal investigations, ILA may collect information relating to:

- allegations;
- evidence;
- interviews;
- witness statements;
- communications;
- findings;
- disciplinary processes; and
- corrective actions.

Investigative information shall be classified according to its sensitivity and accessed only by authorized persons.

PART XIII

DATA COLLECTION DOCUMENTATION

5.34 Data Collection Records

Departments shall maintain appropriate documentation regarding significant data collection activities.

Records may include:

a. purpose of collection;

b. lawful basis;

c. categories of information collected;

d. categories of individuals affected;

e. collection tools used;

f. responsible officers;

g. recipients of information;

h. retention requirements;

i. security measures applied; and

j. relevant approvals.

5.35 Review of Collection Practices

Departments shall periodically review collection practices to ensure:

a. continued necessity;

b. accuracy;

c. compliance with this Policy;

d. reduction of unnecessary information collection;

e. appropriate security controls; and

f. alignment with changing operational requirements.

PART XIV

PROHIBITED DATA COLLECTION PRACTICES

5.36 Prohibited Collection Activities

ILA personnel shall not:

a. collect personal data without a legitimate purpose;

b. collect information unrelated to assigned duties;

c. mislead individuals regarding the purpose of collection;

d. collect unnecessary sensitive personal information;

e. obtain information through intimidation or coercion;

f. secretly record individuals without authorization except where lawful investigative procedures require otherwise;

g. copy or retain personal documents unnecessarily;

h. collect information using unauthorized personal devices or applications;

i. create unofficial databases;

j. collect personal data for personal, political, commercial, or unauthorized purposes; or

k. collect information in a manner likely to expose individuals to harm.

CHAPTER SIX

DATA STORAGE, SECURITY AND ACCESS CONTROL

6.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that effective data protection requires more than lawful collection of information. Personal data must be securely stored, protected against unauthorized access, alteration, disclosure, loss, destruction, or misuse throughout its entire lifecycle.

ILA shall implement appropriate technical, administrative, physical, and organizational safeguards to protect personal data and confidential information against risks arising from human error, negligence, malicious conduct, cyber threats, unauthorized disclosure, theft, loss, and other security incidents.

All employees, volunteers, consultants, interns, partners, and third parties handling ILA information shall comply with the requirements of this Chapter.

PART I

GENERAL DATA SECURITY PRINCIPLES

6.2 Security Obligations

ILA shall ensure that personal data is protected through safeguards appropriate to:

a. the sensitivity and classification of the information;

b. the volume of information processed;

c. the potential harm arising from unauthorized disclosure;

d. the nature of the processing activity;

e. available technological solutions;

f. operational requirements; and

g. legal, contractual, and donor obligations.

Security measures shall be reviewed periodically to ensure continued effectiveness.

6.3 Confidentiality, Integrity and Availability

ILA shall protect information based on three fundamental security objectives:

(a) Confidentiality

Ensuring that personal data is accessible only to authorized persons with a legitimate need to access it.

(b) Integrity

Ensuring that information remains accurate, complete, reliable, and protected against unauthorized alteration or destruction.

(c) Availability

Ensuring that authorized personnel can access necessary information when required for legitimate organizational purposes.

6.4 Security by Risk-Based Approach

Security measures shall be proportionate to identified risks.

Highly Confidential Information shall receive the highest level of protection.

Examples include:

- legal aid case files;
- client communications;
- privileged legal documents;
- safeguarding records;
- PSEA investigations;
- whistleblower information;
- witness information;
- medical records;
- biometric information;
- passwords and security credentials.

PART II

PHYSICAL STORAGE SECURITY

6.5 Paper Records

Physical records containing personal data shall be stored securely and protected against unauthorized access.

Examples include:

- client files;
- personnel files;
- contracts;
- financial documents;
- investigation records;
- beneficiary registration forms;
- signed consent forms; and
- confidential correspondence.

6.6 Physical File Storage Requirements

Departments maintaining physical records shall ensure that:

a. files are stored in secure cabinets or rooms;

b. access is restricted to authorized personnel;

c. confidential files are not left unattended;

d. visitors cannot access confidential documents;

e. files removed from storage are tracked where necessary;

f. sensitive documents are not stored in open areas;

g. documents are protected from fire, water damage, pests, and deterioration; and

h. unauthorized copying or removal is prohibited.

6.7 Legal Files

Legal aid files shall be maintained with heightened confidentiality.

Legal files shall:

a. be assigned appropriate file reference numbers;

b. be stored separately from general administrative records;

c. only be accessed by authorized legal personnel;

d. not be disclosed without proper authorization;

e. be protected against unauthorized copying; and

f. be maintained in accordance with professional legal obligations.

6.8 Transport of Physical Records

Where physical records containing personal information must be transported:

a. transportation shall be authorized;

b. records shall be securely packaged;

c. unnecessary exposure shall be avoided;

d. custody shall be maintained throughout transportation; and

e. loss or unauthorized access shall be reported immediately.

PART III

ELECTRONIC STORAGE SECURITY

6.9 Electronic Information Systems

Electronic personal data shall only be stored using approved organizational systems, including:

- organizational servers;
- approved cloud platforms;
- secure databases;
- approved document management systems;
- authorized computers;
- encrypted storage devices; and

- other ICT-approved solutions.

Personnel shall not store organizational personal data in unauthorized systems.

6.10 Prohibited Electronic Storage

Personnel shall not store Highly Confidential Information:

a. on personal email accounts;

b. on unauthorized cloud storage services;

c. on unprotected personal devices;

d. on publicly accessible platforms;

e. on removable storage devices without authorization;

f. in personal messaging applications without approved safeguards; or

g. in unofficial databases.

PART IV

INFORMATION SECURITY CONTROLS

6.11 Access Control

Access to personal data shall be controlled according to:

a. The person's role;

b. Operational responsibilities;

c. The sensitivity of the information;

d. The principle of least privilege; and

e. Legitimate business need.

No person shall receive access merely because they are employed by ILA.

6.12 Role-Based Access Control

ILA shall implement role-based access controls where technically possible.

Access shall be assigned according to functional responsibilities, including:

Legal Department

May access:

- client files;
- legal documents;
- court records;
- legal correspondence.

Human Resources Department

May access:

- personnel records;
- employment information;
- payroll information.

Finance Department

May access:

- financial records;
- payment information;
- accounting documentation.

MEAL Department

May access:

- monitoring data;
- evaluation information;
- programme statistics.

Safeguarding Personnel

May access:

- safeguarding complaints;
- protection records;
- investigation files.

Access between departments shall be restricted unless there is an approved operational requirement.

6.13 User Accounts

Each authorized user shall have an individual account.

Users shall not:

a. Share passwords;

b. Use another person's account;

c. Allow unauthorized persons to access their account;

d. Create unauthorized accounts; or

e. Bypass security controls.

6.14 Access Review

Department heads shall periodically review user access permissions to ensure that:

a. Access remains necessary;

b. Former employees have been removed;

c. Transferred employees have appropriate access changes;

d. Excessive permissions are removed; and

e. Unauthorized access risks are reduced.

PART V

PASSWORD AND AUTHENTICATION SECURITY

6.15 Password Requirements

ILA shall require strong password practices for all systems containing organizational information.

Passwords shall:

a. Be unique to each user;

b. Not be shared;

c. Not be written in publicly accessible locations;

d. Be changed where compromise is suspected;

e. Comply with ICT security standards.

6.16 Multi-Factor Authentication

Where technically available, ILA shall implement multi-factor authentication for:

a. email systems;

b. cloud storage;

c. financial systems;

d. administrative platforms;

e. databases containing sensitive information; and

f. remote access systems.

PART VI

ENCRYPTION AND SECURE TRANSMISSION

6.17 Encryption

ILA shall use encryption or equivalent security measures where appropriate to protect sensitive information during:

a. Electronic storage;

b. Transmission;

c. Remote access;

d. Backup processes; and

e. Transfer to third parties.

6.18 Transmission of Personal Data

Personnel transmitting personal data shall ensure that:

a. The recipient is authorized;

b. The information is necessary to share;

c. Secure communication channels are used;

d. Unnecessary attachments are avoided;

e. Recipients are verified before sending; and

f. Accidental disclosure risks are minimized.

6.19 Email Security

Employees shall exercise caution when sending information through email.

Before sending confidential information, personnel shall verify:

- recipient identity;
- attachments;
- intended recipients;
- sensitivity level;
- security requirements.

Highly Confidential Information should only be transmitted through approved secure methods

PART VII

BACKUP AND BUSINESS CONTINUITY

6.20 Data Backup

ILA shall maintain appropriate backup arrangements to protect against:

- accidental deletion;
- system failure;
- cyber incidents;
- equipment loss;
- natural disasters; and
- other operational disruptions.

6.21 Backup Requirements

Backups shall:

a. Occur regularly;

b. Be protected against unauthorized access;

c. Be tested periodically;

d. Include critical organizational information;

e. Be stored separately from primary systems where appropriate; and

f. Comply with retention requirements.

6.22 Disaster Recovery

ILA shall maintain procedures for restoring access to essential information following:

- cybersecurity incidents;
- equipment failure;
- physical disasters;
- unauthorized deletion;
- system interruption; or
- other emergencies.

PART VIII

DEVICE SECURITY AND REMOTE WORKING

6.23 Organizational Devices

Any computer, laptop, tablet, mobile phone, storage device, or other electronic equipment provided by ILA or used for official organizational activities shall be treated as an organizational information asset.

Personnel using organizational devices shall ensure that:

a. Devices are used primarily for authorized organizational purposes;

b. Security settings are not disabled;

c. Unauthorized software is not installed;

d. Operating systems and security applications are regularly updated;

e. Devices are protected by passwords or other authentication mechanisms;

f. Confidential information is not exposed to unauthorized persons;

g. Devices are physically secured against loss or theft; and

h. Incidents involving devices are immediately reported.

6.24 Personal Devices

Where employees or consultants use personal devices for organizational work, such use shall only occur where:

a. Authorization has been granted;

b. Appropriate security controls are implemented;

c. Organizational information is stored securely;

d. Access can be removed when required;

e. The device meets minimum security standards; and

f. Confidentiality obligations are maintained.

ILA may restrict or prohibit the use of personal devices where such use creates unacceptable privacy or security risks.

6.25 Mobile Devices

Mobile devices present increased risks due to portability and potential loss.

Personnel using mobile devices for organizational activities shall:

a. Enable device passwords or biometric protection where appropriate;

b. Activate automatic screen locking;

c. Avoid storing unnecessary sensitive information locally;

d. Use approved applications for official communication;

e. Avoid connecting to insecure networks where possible;

f. Report lost or stolen devices immediately; and

g. Permit appropriate security measures where organizational information is stored.

6.26 Lost or Stolen Devices

Where an organizational device or a device containing ILA information is lost, stolen, damaged, or compromised, the user shall immediately notify:

- the ICT Unit;
- their supervisor; and
- the Data Protection Officer where personal data may be affected.

ILA shall assess whether containment measures, remote access removal, data deletion, or breach notification procedures are required.

PART IX

REMOTE WORK AND OFF-SITE ACCESS

6.27 Remote Working Arrangements

Where personnel work remotely or access organizational systems outside ILA premises, they shall maintain the same level of confidentiality and security required within the workplace.

Remote workers shall:

a. use approved systems;

b. protect screens and documents from unauthorized viewing;

c. avoid discussing confidential matters in public places;

d. secure physical documents;

e. use secure internet connections where possible;

f. prevent unauthorized household or third-party access;

g. follow organizational ICT requirements; and

h. promptly report security concerns.

6.28 Public Networks

Personnel shall exercise caution when accessing organizational information through public Wi-Fi networks, shared computers, or other insecure environments.

Highly Confidential Information shall not be accessed through insecure networks unless appropriate security measures are implemented.

PART X

CLOUD STORAGE AND THIRD-PARTY PLATFORMS

6.29 Use of Cloud Services

ILA may use cloud-based systems for storage, collaboration, communication, programme management, and other operational purposes.

Before adopting a cloud service, ILA shall consider:

a. Security features;

b. Confidentiality protections;

c. Access controls;

d. Data location and transfer arrangements;

e. Provider reliability;

f. Contractual protections;

g. Backup arrangements;

h. Breach notification procedures; and

i. Compliance with donor and legal obligations.

6.30 Approved Platforms

Personnel shall only use cloud platforms, software applications, and digital tools approved by ILA.

The use of unauthorized platforms for storing or sharing organizational information is prohibited.

Examples of prohibited practices include:

- uploading client files to personal cloud accounts;
- sharing confidential documents through unauthorized platforms;
- using personal accounts for organizational databases; and
- transferring sensitive information through unapproved applications.

6.31 Third-Party Service Providers

Where third parties process personal data on behalf of ILA, appropriate contractual arrangements shall be established.

Contracts shall, where applicable, require third parties to:

a. process information only according to ILA instructions;

b. maintain confidentiality;

c. implement appropriate security measures;

d. restrict unauthorized access;

e. notify ILA of security incidents;

f. return or securely destroy information when services end; and

g. permit appropriate compliance verification.

PART XI

ACCESS LOGGING AND MONITORING

6.32 Access Monitoring

Where technically feasible, ILA shall maintain records of access to significant information systems containing sensitive personal data.

Monitoring may include:

- user access logs;
- login activity;
- file access records;
- database activity;
- system alerts;
- security events; and
- administrative changes.

6.33 Purpose of Monitoring

Monitoring activities shall be undertaken to:

a. Detect unauthorized access;

b. Investigate security incidents;

c. Support accountability;

d. Protect organizational assets;

e. Comply with legal and donor obligations; and

f. Improve information security.

Monitoring shall not be conducted for unjustified surveillance of employees or beneficiaries.

6.34 Review of Access Records

The ICT Unit and relevant authorized personnel may periodically review access records to identify:

- unusual activity;
- unauthorized access attempts;
- inappropriate access;
- compromised accounts; or
- security weaknesses.

PART XII

CONFIDENTIALITY OBLIGATIONS

6.35 Duty of Confidentiality

All persons handling ILA information have a continuing duty to protect confidentiality during and after their engagement with the Organization.

This obligation applies to:

- employees;
- volunteers;
- interns;
- consultants;
- board members;
- partners;

- contractors; and
- service providers.

6.36 Confidentiality Agreements

Where appropriate, personnel and third parties shall sign confidentiality undertakings confirming their obligation to protect organizational information.

Confidentiality obligations shall include:

a. Prohibition against unauthorized disclosure;

b. Responsible handling of records;

c. Protection of passwords and credentials;

d. Secure disposal requirements;

e. Reporting obligations; and

f. Continuing confidentiality after termination.

6.37 Professional Confidentiality

Personnel engaged in legal services shall comply with applicable professional duties concerning:

- lawyer-client confidentiality;
- legal professional privilege;
- court confidentiality requirements;
- ethical obligations; and
- professional conduct rules.

PART XIII

STAFF RESPONSIBILITIES FOR DATA SECURITY

6.38 Responsibilities of All Personnel

Every person handling ILA information shall:

a. comply with this Policy;

b. protect information entrusted to them;

c. access information only for authorized purposes;

d. maintain confidentiality;

e. report suspected security incidents;

f. follow ICT security procedures;

g. participate in required training;

h. protect organizational devices and documents; and

i. cooperate with investigations.

6.39 Responsibilities of Managers

Managers shall:

a. ensure staff understand their information protection obligations;

b. approve access based on operational need;

c. review access requirements periodically;

d. ensure secure handling of departmental records;

e. identify training needs;

f. report risks and incidents; and

g. support implementation of corrective actions.

6.40 Responsibilities of ICT Unit

The ICT Unit shall:

a. maintain technical security controls;

b. manage user accounts;

c. support secure systems;

d. implement updates and security improvements;

e. monitor cybersecurity risks;

f. support incident response;

g. maintain backups;

h. advise departments on technology risks; and

i. implement appropriate technical safeguards.

PART XIV

SECURITY TRAINING AND AWARENESS

6.41 Training Requirements

ILA shall provide appropriate training to personnel who handle personal data.

Training shall address:

- confidentiality obligations;
- information security practices;
- password management;
- phishing awareness;
- data breach reporting;
- safe handling of sensitive information;
- safeguarding confidentiality;
- legal professional privilege; and
- responsibilities under this Policy.

6.42 Periodic Awareness Activities

ILA may conduct:

a. refresher training;

b. security awareness sessions;

c. information notices;

d. simulated security exercises;

e. policy briefings; and

f. targeted training for high-risk roles.

PART XV

REVIEW AND IMPROVEMENT OF SECURITY CONTROLS

6.43 Security Reviews

ILA shall periodically assess whether its security measures remain appropriate considering:

a. emerging threats;

b. technological developments;

c. operational changes;

d. audit findings;

e. incident lessons learned;

f. donor requirements; and

g. changes in legal obligations.

6.44 Corrective Measures

Where security weaknesses are identified, ILA shall implement appropriate corrective measures, including:

- system improvements;
- additional controls;
- staff training;
- access restrictions;
- policy updates;
- disciplinary measures where appropriate; and
- enhanced monitoring.

6.45 Continuous Improvement

Data security shall be treated as an ongoing organizational responsibility.

ILA shall continually strengthen its information security framework to ensure that personal data remains protected against evolving risks.

CHAPTER SEVEN

DATA SHARING, DISCLOSURE AND TRANSFER OF PERSONAL DATA

7.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that responsible information sharing is essential for effective legal assistance, protection services, programme implementation, accountability, research, partnerships, and institutional coordination.

However, sharing personal data creates risks to individual privacy, confidentiality, safety, dignity, and legal rights. Unauthorized disclosure may expose individuals to retaliation, discrimination, legal harm, security threats, or other adverse consequences.

Accordingly, ILA shall ensure that all sharing, disclosure, transfer, or release of personal data is:

a. lawful;

b. necessary;

c. proportionate;

d. purpose-specific;

e. limited to authorized recipients;

f. appropriately documented; and

g. conducted using adequate safeguards.

No personal data shall be shared merely because a request has been made or because access appears convenient.

PART I

GENERAL PRINCIPLES FOR DATA SHARING

7.2 Data Sharing Principles

All decisions to share personal data shall be guided by the following principles:

(a) Necessity

Information shall only be shared where there is a genuine operational, legal, safeguarding, contractual, or public interest need.

(b) Proportionality

The amount of information shared shall be limited to what is necessary to achieve the intended purpose.

(c) Purpose Limitation

Information shall only be shared for the purpose for which it was collected or another compatible lawful purpose.

(d) Confidentiality

Recipients shall be required to protect information received and prevent unauthorized disclosure.

(e) Accountability

ILA shall maintain appropriate records demonstrating why information was shared, with whom, and under what authority.

7.3 Authorization Before Sharing

Before sharing personal data, personnel shall confirm:

a. the identity of the recipient;

b. the purpose of sharing;

c. the lawful basis permitting disclosure;

d. whether the individual has been informed or consented where required;

e. whether the disclosure creates risks to the individual;

f. whether less information could achieve the purpose; and

g. whether appropriate safeguards are in place.

Where uncertainty exists, personnel shall seek guidance from the Data Protection Officer, Legal Unit, or authorized management personnel.

PART II

INTERNAL DATA SHARING

7.4 Sharing Between Departments

ILA may share personal data internally where such sharing is necessary for legitimate organizational functions.

Internal sharing may include:

- Legal Department accessing client information for legal representation;
- Finance Department accessing payment information for financial administration;
- Human Resources accessing personnel records for employment management;
- MEAL Department accessing programme information for monitoring and evaluation;
- Safeguarding personnel accessing protection information for case management.

7.5 Need-to-Know Principle

Internal access shall be based on the principle that personnel should only receive information necessary to perform their assigned responsibilities.

Employment with ILA does not automatically grant access to all organizational information.

7.6 Internal Restrictions

Personnel shall not:

a. access information out of curiosity;

b. share information informally with colleagues who have no operational need;

c. discuss confidential matters in public areas;

d. copy files unnecessarily;

e. transfer information between departments without authorization; or

f. use information obtained through work for personal purposes.

PART III

SHARING WITH EXTERNAL PARTIES

7.7 General Rule

ILA shall only share personal data with external persons or organizations where:

a. there is a lawful basis;

b. the disclosure serves a legitimate purpose;

c. the recipient requires the information;

d. appropriate safeguards exist; and

e. the disclosure does not create unacceptable risks.

External recipients may include:

- government institutions;
- courts;
- donors;
- implementing partners;
- referral organizations;
- professional advisers;
- auditors;
- researchers;
- service providers; and
- regulatory authorities.

7.8 Due Diligence Before External Sharing

Before sharing information with an external party, ILA shall assess:

a. the identity and reliability of the recipient;

b. the recipient's ability to protect information;

c. confidentiality obligations;

d. security measures available;

e. the sensitivity of the information;

f. potential risks to affected individuals; and

g. whether a written agreement is required.

PART IV

DATA SHARING AGREEMENTS

7.9 Requirement for Agreements

Where ILA regularly shares personal data with external organizations, a written agreement shall ordinarily be established.

Data-sharing agreements may include:

a. purpose of sharing;

b. categories of information shared;

c. categories of individuals affected;

d. responsibilities of each party;

e. security requirements;

f. confidentiality obligations;

g. restrictions on further disclosure;

h. retention and deletion requirements;

i. breach notification obligations;

j. monitoring and compliance arrangements; and

k. dispute resolution mechanisms.

7.10 Partner Organizations

Where ILA works with implementing partners, consortium members, community organizations, or referral institutions, personal data sharing shall be governed by appropriate partnership agreements, memoranda of understanding, or data-sharing arrangements.

Partners shall not use ILA-provided information for unrelated purposes.

PART V

DISCLOSURE TO GOVERNMENT AUTHORITIES AND COURTS

7.11 Government Requests

ILA may disclose personal data to government authorities where:

a. disclosure is legally required;

b. necessary for safeguarding;

c. required for legal proceedings;

d. authorized by the individual;

e. necessary to prevent serious harm; or

f. otherwise permitted by law.

Before responding to government requests, ILA shall verify:

- the identity of the requesting authority;
- the legal basis for the request;
- the scope of information requested; and
- whether disclosure is limited to necessary information.

7.12 Court Orders

Where a court or competent authority orders disclosure of personal information, ILA shall:

a. verify the authenticity of the order;

b. assess applicable confidentiality obligations;

c. consult legal counsel where appropriate;

d. disclose only the information required;

e. maintain records of the disclosure; and

f. consider whether any legal privilege or protection applies.

PART VI

LEGAL PROFESSIONAL PRIVILEGE AND CONFIDENTIALITY

7.13 Protection of Legal Information

Information obtained or created in connection with legal representation shall receive enhanced protection.

ILA shall not disclose privileged legal information except:

a. with informed client authorization;

b. where disclosure is required by law after appropriate review;

c. pursuant to a valid court order;

d. where privilege has been waived; or

e. under other legally recognized exceptions.

7.14 Client Consent for Disclosure

Where disclosure of client information is not otherwise legally authorized, ILA shall obtain informed consent before sharing client information with third parties.

Consent shall specify:

a. what information will be disclosed;

b. the recipient;

c. the purpose of disclosure;

d. potential consequences; and

e. the individual's right to refuse.

PART VII

SAFEGUARDING AND PROTECTION-RELATED DISCLOSURES

7.15 Safeguarding Exceptions

In exceptional circumstances, ILA may disclose personal information without consent where necessary to:

a. protect a child from harm;

b. prevent serious injury or death;

c. respond to safeguarding concerns;

d. comply with mandatory reporting obligations; or

e. protect another person's fundamental rights.

7.16 Minimum Necessary Disclosure

Even where disclosure is justified, ILA shall:

a. disclose only necessary information;

b. consider risks to the affected individual;

c. select appropriate recipients;

d. document the decision; and

e. maintain confidentiality after disclosure.

PART VIII

DONOR AND PUBLIC REPORTING

7.17 Donor Reporting

ILA may share programme information with donors where required under grant agreements or accountability obligations.

However:

a. personal identifiers shall be removed wherever possible;

b. case examples shall be anonymized unless consent exists;

c. sensitive information shall not be unnecessarily disclosed;

d. safeguarding information shall receive special protection; and

e. donor confidentiality obligations shall be respected.

7.18 Public Communications

Before publishing information through:

- websites;
- reports;
- social media;
- press releases;
- newsletters;
- advocacy materials; or
- public campaigns,

ILA shall ensure that:

a. publication is authorized;

b. individuals cannot be identified unnecessarily;

c. consent has been obtained where required;

d. vulnerable persons are protected; and

e. publication does not create security risks.

PART IX

RESEARCH, ACADEMIC AND POLICY DATA SHARING

7.19 Research Data Sharing

ILA may share research, monitoring, evaluation, learning, and policy-related information with academic institutions, researchers, consortium partners, donors, and other legitimate stakeholders where such sharing supports lawful organizational objectives.

Before sharing research-related information, ILA shall ensure that:

a. the purpose of sharing is clearly defined;

b. personal identifiers are removed where possible;

c. participants' confidentiality is protected;

d. ethical requirements have been considered;

e. the recipient has appropriate safeguards;

f. further disclosure is restricted; and

g. applicable agreements are established where necessary.

7.20 Academic Collaborations

Where ILA collaborates with universities, research institutions, or individual researchers, arrangements shall address:

a. ownership of research data;

b. confidentiality obligations;

c. permitted uses of information;

d. publication requirements;

e. anonymization standards;

f. storage and retention arrangements;

g. security responsibilities; and

h. destruction or return of information after completion.

Researchers shall not publish information that may identify beneficiaries, clients, witnesses, survivors, or vulnerable individuals without lawful authorization.

PART X

SERVICE PROVIDERS AND DATA PROCESSORS

7.21 Use of Data Processors

ILA may engage third-party service providers who process personal data on behalf of the Organization.

Examples include:

- cloud service providers;
- ICT support providers;
- payroll service providers;
- auditors;
- consultants;
- survey organizations;
- database management providers;
- legal experts;
- translation services; and
- other technical service providers.

7.22 Processor Obligations

Before allowing a third party to process personal data, ILA shall ensure that the provider:

a. acts only on documented instructions from ILA;

b. maintains confidentiality;

c. implements appropriate security measures;

d. restricts access to authorized personnel;

e. does not use information for unrelated purposes;

f. reports suspected breaches promptly;

g. assists ILA in responding to data subject requests where applicable;

h. returns or securely deletes information after completion of services; and

i. complies with applicable contractual obligations.

7.23 Vendor Due Diligence

Before engaging a service provider, ILA shall consider:

a. the nature of information to be processed;

b. the provider's security capability;

c. confidentiality arrangements;

d. technical safeguards;

e. reputation and reliability;

f. location of data processing;

g. breach management procedures; and

h. compliance with donor or legal requirements.

PART XI

CROSS-BORDER TRANSFER OF PERSONAL DATA

7.24 General Principle

ILA recognizes that personal data may sometimes need to be transferred outside South Sudan for legitimate operational purposes, including:

- donor reporting;
- international partnerships;
- cloud storage;
- technical support;
- research collaboration;
- legal networks;
- humanitarian coordination; and
- organizational administration.

Such transfers shall only occur where adequate safeguards are implemented.

7.25 Assessment Before Transfer

Before transferring personal data outside South Sudan, ILA shall assess:

a. the purpose of transfer;

b. the categories and sensitivity of information;

c. the destination country or organization;

d. available privacy protections;

e. contractual safeguards;

f. potential risks to individuals; and

g. whether the transfer is necessary.

7.26 Safeguards for International Transfers

Appropriate safeguards may include:

a. written data-sharing agreements;

b. confidentiality agreements;

c. contractual restrictions on further disclosure;

d. encryption;

e. access restrictions;

f. anonymization or pseudonymization;

g. secure transfer mechanisms; and

h. verification of recipient security practices.

7.27 High-Risk Transfers

Transfers involving the following information require enhanced review:

- legal aid client files;
- privileged legal documents;
- safeguarding records;
- child protection information;
- witness information;
- whistleblower information;
- medical information; and
- investigation records.

Such transfers require authorization from appropriate management and, where necessary, the Legal Unit or Data Protection Officer.

PART XII

SHARING WITH INTERNATIONAL ORGANIZATIONS AND DONORS

7.28 International Partners

Where ILA shares information with international organizations, United Nations agencies, international NGOs, or foreign institutions, the Organization shall ensure that:

a. the purpose of sharing is documented;

b. responsibilities are clearly defined;

c. confidentiality obligations exist;

d. security safeguards are adequate;

e. vulnerable persons are protected; and

f. information is not further disclosed without authorization.

7.29 Donor Compliance Requirements

Where donor agreements require reporting involving personal information, ILA shall seek to satisfy accountability requirements while protecting individual privacy.

ILA shall prioritize:

a. anonymized reporting;

b. aggregated statistics;

c. coded case information;

d. restricted access to detailed information; and

e. disclosure only where necessary.

PART XIII

EMERGENCY INFORMATION SHARING

7.30 Emergency Situations

In urgent circumstances, ILA may share personal data where necessary to:

a. protect life;

b. prevent serious harm;

c. provide emergency assistance;

d. facilitate protection services;

e. respond to security incidents;

f. support evacuation or relocation; or

g. comply with emergency legal obligations.

7.31 Emergency Disclosure Safeguards

Even during emergencies, personnel shall:

a. verify the recipient where possible;

b. share only necessary information;

c. consider risks to the affected person;

d. record the disclosure;

e. notify responsible management where appropriate; and

f. apply confidentiality safeguards after disclosure.

Emergency circumstances do not justify unrestricted sharing of personal information.

PART XIV

RECORDING AND TRACKING DISCLOSURES

7.32 Disclosure Register

ILA shall maintain appropriate records of significant disclosures of personal data.

The disclosure register may include:

a. date of disclosure;

b. information disclosed;

c. purpose of disclosure;

d. lawful basis;

e. recipient;

f. approving officer;

g. safeguards applied;

h. whether consent was obtained; and

i. follow-up actions required.

7.33 Accountability Records

Documentation of disclosures shall support:

- internal accountability;
- audits;
- donor compliance;
- legal review;
- incident investigations; and
- improvement of information-sharing practices.

PART XV

UNAUTHORIZED DISCLOSURE RESPONSE

7.34 Unauthorized Disclosure

Unauthorized disclosure includes:

a. sending information to the wrong recipient;

b. accidental publication;

c. sharing information without authorization;

d. discussing confidential matters improperly;

e. loss of confidential documents;

f. unauthorized copying; or

g. access by persons without permission.

7.35 Immediate Reporting

Any person who becomes aware of unauthorized disclosure shall immediately report the incident in accordance with the Data Breach Management Procedure.

Failure to report a known disclosure may constitute a violation of this Policy.

7.36 Investigation and Remedial Action

ILA shall assess unauthorized disclosures and determine:

a. the information affected;

b. persons affected;

c. the cause of disclosure;

d. potential harm;

e. containment measures;

f. notification requirements;

g. corrective action; and

h. disciplinary implications where applicable.

PART XVI

PROHIBITED DATA SHARING PRACTICES

7.37 Prohibited Disclosure

ILA personnel shall not:

a. share personal data without authorization;

b. disclose client information for personal reasons;

c. share confidential information through informal channels;

d. provide information to unauthorized persons;

e. publish identifying information without approval;

f. transfer information to personal accounts;

g. disclose information obtained through legal representation improperly;

h. share safeguarding information unnecessarily;

i. disclose whistleblower identities without authorization;

j. provide information to media without approval; or

k. use organizational information for personal, political, commercial, or unlawful purposes.

CHAPTER EIGHT

DATA SUBJECT RIGHTS AND REQUEST MANAGEMENT

8.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that individuals whose personal data is processed have important rights regarding the collection, use, storage, disclosure, and protection of their information.

ILA is committed to respecting these rights and ensuring that individuals can exercise meaningful control over their personal data, subject to lawful limitations arising from legal obligations, professional confidentiality, safeguarding requirements, security considerations, and the legitimate interests of other persons.

All requests relating to personal data shall be handled fairly, transparently, securely, and within a reasonable timeframe.

PART I

GENERAL PRINCIPLES RELATING TO DATA SUBJECT RIGHTS

8.2 Recognition of Individual Rights

Any identified or identifiable individual whose personal data is processed by ILA (referred to in this Policy as a **Data Subject**) may exercise applicable rights concerning their personal information.

These rights apply to:

a. legal aid clients;

b. beneficiaries;

c. programme participants;

d. employees;

e. volunteers;

f. interns;

g. consultants;

h. complainants;

i. witnesses;

j. research participants;

k. partners; and

l. other individuals whose information is processed by ILA.

8.3 Limitations on Rights

Data subject rights shall be exercised subject to applicable legal, ethical, and operational limitations.

ILA may restrict or refuse a request where necessary to protect:

a. legal professional privilege;

b. confidentiality obligations;

c. rights of other individuals;

d. safeguarding considerations;

e. ongoing investigations;

f. legitimate legal proceedings;

g. security interests;

h. fraud prevention measures;

i. donor confidentiality obligations; or

j. statutory obligations.

Any refusal or restriction shall be justified and documented.

8.4 Fair and Transparent Handling

ILA shall ensure that:

a. requests are handled without discrimination;

b. individuals are not required to provide unnecessary information;

c. responses are communicated clearly;

d. decisions are documented;

e. confidentiality is maintained throughout the process; and

f. individuals are informed of available complaint mechanisms where requests are denied.

PART II

RIGHT TO INFORMATION AND TRANSPARENCY

8.5 Right to Information

Individuals have the right to receive clear information regarding how ILA processes their personal data.

ILA shall provide information concerning:

a. the identity and contact details of ILA;

b. purposes of processing;

c. categories of information collected;

d. lawful basis for processing;

e. recipients of information;

f. retention periods;

g. security measures;

h. available rights;

i. complaint procedures; and

j. circumstances where information may be disclosed.

8.6 Privacy Notices

ILA shall provide privacy notices through appropriate channels, including:

- client intake materials;
- beneficiary registration forms;
- employment documents;
- research materials;
- website notices;

- consent forms; and
- programme documentation.

Privacy notices shall be reviewed periodically to ensure accuracy.

PART III

RIGHT OF ACCESS

8.7 Right to Access Personal Data

Individuals have the right to request confirmation of whether ILA processes their personal data and, where applicable, request access to such information.

Access requests may relate to:

a. personal details;

b. beneficiary records;

c. employment information;

d. communications;

e. programme participation information;

f. research data; and

g. other personal information held by ILA.

8.8 Access Request Procedure

Individuals requesting access shall:

a. submit the request through approved channels;

b. provide sufficient information to enable identification;

c. specify the information requested where possible;

d. cooperate with verification procedures; and

e. allow reasonable time for processing.

8.9 Identity Verification

Before providing access, ILA shall verify the identity of the requester to prevent unauthorized disclosure.

Verification measures may include:

- identification documents;
- confirmation through known contact details;
- security questions;
- authorized representatives;
- other appropriate verification methods.

8.10 Access to Legal Files

Requests involving legal aid files shall be assessed carefully considering:

a. lawyer-client confidentiality;

b. legal professional privilege;

c. rights of other parties;

d. court confidentiality requirements;

e. ongoing litigation; and

f. investigative considerations.

Access may be provided subject to lawful restrictions.

PART IV

RIGHT TO CORRECTION

8.11 Right to Rectification

Individuals have the right to request correction of inaccurate, incomplete, outdated, or misleading personal information held by ILA.

Upon receiving a correction request, ILA shall:

a. assess the accuracy of the information;

b. verify supporting evidence where necessary;

c. update records where appropriate;

d. record the correction; and

e. notify relevant recipients where correction is required.

8.12 Accuracy of Legal Records

Where information forms part of legal records, court documents, investigation records, or professional opinions, correction shall not involve altering historical records improperly.

Instead, ILA may:

a. add clarification;

b. record the individual's disagreement;

c. attach supplementary information; or

d. preserve the original record with appropriate annotation.

PART V

RIGHT TO DELETION OR ERASURE

8.13 Right to Request Deletion

Individuals may request deletion of their personal data where:

a. the information is no longer necessary;

b. processing was based solely on consent and consent has been withdrawn;

c. processing was unlawful;

d. deletion is required by law; or

e. retention is no longer justified.

8.14 Limitations on Deletion

ILA may refuse deletion where retention is necessary for:

a. legal proceedings;

b. professional obligations;

c. safeguarding purposes;

d. audit requirements;

e. donor obligations;

f. statutory record keeping;

g. establishment or defense of legal claims; or

h. preservation of evidence.

8.15 Secure Disposal Following Approval

Where deletion is approved, ILA shall ensure that information is securely destroyed through appropriate methods, including:

- secure digital deletion;
- destruction of paper records;
- removal from active systems;
- deletion from backups where technically possible; and
- confirmation of disposal.

PART VI

RIGHT TO RESTRICT PROCESSING

8.16 Restriction Requests

Individuals may request restriction of processing where:

a. accuracy of information is disputed;

b. processing is unlawful but deletion is not requested;

c. information is required for legal claims; or

d. the individual objects to processing pending review.

8.17 Effect of Restriction

Where processing is restricted:

a. information shall remain stored securely;

b. further use shall cease except where legally permitted;

c. authorized personnel shall be informed;

d. restrictions shall be recorded; and

e. the individual shall be informed when restriction is lifted.

PART VII

RIGHT TO OBJECT

8.18 Right to Object

Individuals may object to certain processing activities where they believe the processing unfairly affects their rights or interests.

ILA shall consider objections relating to:

a. processing based on legitimate interests;

b. direct communications;

c. research activities; or

d. other non-mandatory processing activities.

8.19 Assessment of Objections

Upon receiving an objection, ILA shall assess:

a. the purpose of processing;

b. the lawful basis relied upon;

c. the impact on the individual;

d. organizational interests;

e. legal obligations; and

f. available alternatives.

ILA shall communicate the outcome and reasons for the decision.

PART VIII

RIGHTS RELATING TO AUTOMATED DECISION-MAKING AND PROFILING

8.20 Automated Decision-Making

ILA recognizes that individuals may be affected by decisions made through automated systems or technology-assisted processes.

Where ILA uses automated tools that produce decisions affecting individuals, the Organization shall ensure that:

a. the purpose of automation is clearly defined;

b. appropriate human oversight exists where necessary;

c. decisions are not based on inaccurate or unfair information;

d. individuals are informed where automated processing significantly affects them; and

e. appropriate safeguards exist against discriminatory or harmful outcomes.

8.21 Automated Profiling

Where ILA conducts profiling or analysis of personal data for legitimate purposes, including programme planning, research, risk assessment, or service delivery, it shall ensure that:

a. the purpose is lawful and documented;

b. unnecessary personal identifiers are avoided;

c. individuals are not unfairly disadvantaged;

d. sensitive personal data is protected;

e. results are reviewed appropriately; and

f. decisions involving significant consequences are subject to human review.

PART IX

RIGHTS OF CLIENTS, BENEFICIARIES AND VULNERABLE PERSONS

8.22 Enhanced Protection for Vulnerable Individuals

ILA shall take additional measures to ensure that vulnerable persons can effectively exercise their data rights.

This includes:

a. using understandable language;

b. providing assistance where literacy or disability creates barriers;

c. avoiding procedures that create additional risks;

d. protecting individuals from retaliation;

e. considering safeguarding concerns; and

f. ensuring confidentiality throughout the process.

8.23 Legal Aid Client Rights

Clients receiving legal assistance from ILA may request information concerning their personal data, subject to:

a. lawyer-client confidentiality;

b. legal professional privilege;

c. court restrictions;

d. rights of other parties;

e. ongoing legal proceedings; and

f. ethical obligations applicable to legal practitioners.

ILA shall balance transparency with its duty to protect confidential legal information.

8.24 Beneficiary Rights

Programme beneficiaries shall have access to appropriate mechanisms to:

a. understand how their information is used;

b. request correction of inaccurate information;

c. raise concerns about misuse of information;

d. submit complaints;

e. request review of decisions involving their information; and

f. receive appropriate explanations.

PART X

AUTHORIZED REPRESENTATIVES

8.25 Requests Through Representatives

A data subject may authorize another person to submit a request on their behalf where appropriate.

Examples may include:

- legal representatives;
- guardians;
- parents or caregivers;
- authorized family members;
- appointed representatives.

8.26 Verification of Representatives

Before responding to a request made by another person, ILA shall verify:

a. the identity of the representative;

b. the authority to act;

c. the identity of the data subject;

d. the scope of authorization; and

e. whether disclosure to the representative is appropriate.

8.27 Children and Persons Lacking Capacity

Where a child or person lacks sufficient capacity to exercise their rights independently, ILA shall consider:

a. the best interests of the individual;

b. applicable legal requirements;

c. safeguarding considerations;

d. the authority of the person making the request; and

e. confidentiality obligations.

PART XI

REQUEST SUBMISSION AND MANAGEMENT PROCEDURE

8.28 Submission of Requests

Requests relating to personal data may be submitted through:

a. written applications;

b. designated email addresses;

c. organizational complaint mechanisms;

d. legal aid offices;

e. human resources channels; or

f. other approved communication channels.

8.29 Minimum Information Required

A request should include:

a. the name of the requester;

b. contact details;

c. description of the request;

d. relevant information to identify records;

e. proof of identity where required; and

f. authority documents where acting on behalf of another person.

ILA shall not require unnecessary information.

8.30 Request Registration

All significant requests shall be recorded in a Data Subject Request Register.

The register shall include:

a. date received;

b. requester details;

c. nature of request;

d. responsible department;

e. verification status;

f. decision made;

g. response date;

h. reasons for refusal or restriction where applicable; and

i. follow-up actions.

PART XII

RESPONSE TIMELINES

8.31 Timely Response

ILA shall respond to data subject requests within a reasonable timeframe considering:

a. complexity of the request;

b. volume of information involved;

c. need for consultation;

d. legal restrictions;

e. safeguarding concerns; and

f. verification requirements.

8.32 Extension of Time

Where a request cannot reasonably be completed within the normal response period, ILA may extend the timeframe where necessary.

The requester shall be informed of:

a. the reason for delay;

b. the expected completion date; and

c. any additional information required.

PART XIII

FEES AND COSTS

8.33 No Unreasonable Charges

ILA shall not impose unreasonable charges for exercising data protection rights.

Requests shall ordinarily be processed without charge.

8.34 Exceptional Administrative Costs

Where permitted, ILA may charge reasonable administrative costs for:

a. repeated excessive requests;

b. clearly unreasonable requests;

c. extensive reproduction of records; or

d. additional services requested beyond normal obligations.

Any such charge shall be justified and approved.

PART XIV

REFUSAL OR RESTRICTION OF REQUESTS

8.35 Grounds for Refusal

ILA may refuse or restrict a request where:

a. the requester cannot be verified;

b. disclosure would violate another person's rights;

c. legal privilege applies;

d. disclosure would prejudice an investigation;

e. retention is required by law;

f. disclosure creates safeguarding risks;

g. the request is manifestly unreasonable; or

h. no personal data exists.

8.36 Communication of Refusal

Where ILA refuses or restricts a request, it shall:

a. provide reasons where appropriate;

b. explain available review mechanisms;

c. identify applicable limitations;

d. maintain confidentiality; and

e. document the decision.

PART XV

COMPLAINTS AND APPEALS MECHANISM

8.37 Right to Complain

Individuals who believe that their data protection rights have not been respected may submit complaints to ILA.

Complaints may relate to:

- unlawful processing;
- refusal of access;
- inaccurate information;
- unauthorized disclosure;
- excessive collection;
- failure to protect information;
- improper refusal of requests; or
- other privacy concerns.

8.38 Internal Review

Complaints shall be reviewed through an appropriate internal mechanism involving:

a. the Data Protection Officer;

b. relevant department heads;

c. the Legal Unit where necessary; or

d. senior management.

8.39 Independent Review

Where appropriate, individuals may be informed of available external remedies, including competent authorities, courts, or other lawful complaint mechanisms.

PART XVI

PROTECTION AGAINST RETALIATION

8.40 Non-Retaliation Principle

ILA shall not retaliate against any person for:

a. exercising data protection rights;

b. requesting access to information;

c. correcting inaccurate information;

d. raising privacy concerns;

e. submitting complaints; or

f. cooperating with privacy investigations.

8.41 Confidential Handling of Requests

Requests and complaints shall be handled confidentially.

Information concerning a request shall only be shared with persons who require access for legitimate processing purposes.

PART XVII

RECORD KEEPING AND CONTINUOUS IMPROVEMENT

8.42 Data Subject Request Records

ILA shall maintain records necessary to demonstrate compliance with this Chapter.

Records may include:

a. submitted requests;

b. decisions made;

c. communications;

d. supporting documents;

e. review outcomes;

f. corrective actions; and

g. lessons learned.

8.43 Monitoring and Improvement

ILA shall periodically review data subject request trends to:

a. identify recurring concerns;

b. improve privacy notices;

c. strengthen collection procedures;

d. improve staff training;

e. enhance accountability mechanisms; and

f. reduce unnecessary processing risks.

CHAPTER NINE

DATA PROTECTION GOVERNANCE AND RESPONSIBILITIES

9.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that effective protection of personal data requires clear accountability, defined responsibilities, adequate resources, and coordinated implementation across the Organization.

Data protection is a shared organizational responsibility and shall not be limited to one department or individual.

Every person who collects, accesses, uses, stores, transfers, or otherwise handles personal data has a responsibility to protect it in accordance with this Policy.

PART I

DATA PROTECTION GOVERNANCE FRAMEWORK

9.2 Governance Structure

ILA’s data protection governance framework shall consist of:

a. Board of Directors;

b. Executive Director;

c. Data Protection Officer;

d. Legal Department;

e. ICT Unit;

f. Human Resources Department;

g. Programme Departments;

h. Monitoring, Evaluation, Accountability and Learning (MEAL) Unit;

i. Safeguarding Unit;

j. Finance and Administration Department;

k. Records Management Function; and

l. All employees and affiliated personnel.

9.3 Accountability Principle

ILA shall maintain clear accountability for:

a. compliance with data protection requirements;

b. implementation of security measures;

c. protection of confidential information;

d. management of data risks;

e. response to incidents;

f. staff awareness; and

g. continuous improvement.

PART II

BOARD OF DIRECTORS RESPONSIBILITIES

9.4 Role of the Board

The Board of Directors shall provide strategic oversight and governance direction regarding data protection.

9.5 Responsibilities of the Board

The Board shall:

a. approve the Data Protection and Privacy Policy;

b. provide oversight on privacy risks;

c. ensure adequate organizational commitment to data protection;

d. receive reports on significant data protection issues;

e. ensure accountability mechanisms exist;

f. support ethical handling of personal information;

g. consider data protection risks in strategic decisions; and

h. promote a culture of confidentiality and accountability.

PART III

EXECUTIVE DIRECTOR RESPONSIBILITIES

9.6 Role of Executive Director

The Executive Director shall have overall responsibility for ensuring implementation of this Policy throughout ILA.

9.7 Responsibilities of Executive Director

The Executive Director shall:

a. ensure adequate resources for data protection;

b. approve necessary procedures and controls;

c. appoint responsible officers where required;

d. ensure compliance across departments;

e. oversee significant data protection risks;

f. ensure appropriate response to serious breaches;

g. promote staff awareness;

h. support accountability measures; and

i. report significant issues to the Board.

PART IV

DATA PROTECTION OFFICER

9.8 Appointment of Data Protection Officer

ILA shall designate a Data Protection Officer (DPO) or responsible data protection focal person to coordinate implementation of this Policy.

The DPO shall have sufficient authority, independence, and access to information necessary to perform assigned responsibilities.

9.9 Responsibilities of Data Protection Officer

The DPO shall:

a. monitor compliance with this Policy;

b. advise management and departments;

c. provide guidance on data protection obligations;

d. review high-risk processing activities;

e. support privacy impact assessments;

f. advise on data-sharing arrangements;

g. coordinate breach response;

h. maintain data protection records;

i. support staff training;

j. monitor data subject requests;

k. promote privacy awareness;

l. review security practices; and

m. recommend improvements.

9.10 Independence of Data Protection Officer

The DPO shall be able to perform duties objectively and shall not be improperly influenced in matters relating to data protection.

The DPO shall have direct access to senior management on significant privacy and security matters.

PART V

LEGAL DEPARTMENT RESPONSIBILITIES

9.11 Role of Legal Department

The Legal Department shall provide legal guidance regarding:

a. confidentiality obligations;

b. legal professional privilege;

c. contractual data protection requirements;

d. court-related disclosures;

e. regulatory obligations;

f. client information protection; and

g. legal risks arising from data processing.

9.12 Legal Department Duties

The Legal Department shall:

a. review data-sharing agreements;

b. advise on lawful disclosures;

c. protect privileged information;

d. support breach investigations;

e. advise on litigation-related retention;

f. review privacy clauses in contracts; and

g. support compliance with professional obligations.

PART VI

ICT UNIT RESPONSIBILITIES

9.13 Role of ICT Unit

The ICT Unit shall be responsible for maintaining technical safeguards that protect organizational information systems.

9.14 ICT Responsibilities

The ICT Unit shall:

a. implement cybersecurity controls;

b. manage user accounts;

c. enforce access restrictions;

d. maintain system security;

e. support encryption and backups;

f. monitor security risks;

g. respond to technical incidents;

h. maintain system updates;

i. support secure disposal of electronic records;

j. advise on technology risks; and

k. maintain ICT security procedures.

PART VII

HUMAN RESOURCES DEPARTMENT RESPONSIBILITIES

9.15 Role of Human Resources

HR shall ensure that personnel understand and comply with their data protection responsibilities.

9.16 HR Responsibilities

HR shall:

a. include confidentiality obligations in employment agreements;

b. maintain secure employee records;

c. ensure staff receive data protection training;

d. manage access changes upon employment changes;

e. support disciplinary processes;

f. protect personnel information;

g. maintain recruitment confidentiality; and

h. support employee exit procedures.

PART VIII

PROGRAMME DEPARTMENT RESPONSIBILITIES

9.17 Programme Data Responsibilities

Programme departments collecting or using personal data shall ensure:

a. lawful collection;

b. informed communication with participants;

c. secure handling of records;

d. appropriate access restrictions;

e. responsible sharing practices;

f. accurate documentation;

g. safeguarding considerations; and

h. timely reporting of incidents.

PART IX

MEAL UNIT RESPONSIBILITIES

9.18 MEAL Data Protection Responsibilities

The MEAL Unit shall ensure that monitoring, evaluation, research, and learning activities comply with this Policy.

9.19 MEAL Duties

The MEAL Unit shall:

a. protect participant information;

b. minimize unnecessary collection;

c. anonymize data where possible;

d. maintain secure databases;

e. protect survey information;

f. ensure ethical research practices;

g. manage data quality responsibly; and

h. coordinate appropriate reporting.

PART X

SAFEGUARDING UNIT RESPONSIBILITIES

9.20 Safeguarding Data Protection Responsibilities

The Safeguarding Unit shall ensure enhanced protection of safeguarding-related information.

9.21 Safeguarding Duties

The Safeguarding Unit shall:

a. protect survivor confidentiality;

b. restrict access to sensitive records;

c. apply survivor-centred information practices;

d. manage safeguarding disclosures carefully;

e. coordinate secure referrals;

f. maintain confidential records;

g. report risks appropriately; and

h. ensure compliance with safeguarding standards.

PART XI

FINANCE AND ADMINISTRATION DEPARTMENT RESPONSIBILITIES

9.22 Role of Finance and Administration Department

The Finance and Administration Department shall ensure that financial, procurement, administrative, and operational records containing personal data are managed securely and responsibly.

9.23 Finance and Administration Duties

The Finance and Administration Department shall:

a. maintain secure financial records;

b. protect supplier, contractor, and employee information;

c. ensure confidentiality of payroll information;

d. restrict access to financial databases;

e. support secure document storage;

f. ensure procurement records are appropriately protected;

g. support secure disposal of administrative records;

h. ensure third-party service providers comply with confidentiality obligations; and

i. report suspected breaches involving administrative information.

PART XII

RECORDS MANAGEMENT RESPONSIBILITIES

9.24 Role of Records Management Function

The Records Management Function shall ensure that organizational records containing personal data are properly created, classified, stored, retained, accessed, and disposed of.

9.25 Records Management Duties

Records management personnel shall:

a. maintain appropriate filing systems;

b. classify records according to sensitivity;

c. implement retention schedules;

d. support secure archiving;

e. control access to physical records;

f. coordinate secure disposal;

g. maintain records inventories;

h. prevent unauthorized removal of documents; and

i. support audits and compliance reviews.

PART XIII

DEPARTMENTAL DATA OWNERS

9.26 Appointment of Data Owners

Each department handling personal data shall designate a responsible officer to serve as a Departmental Data Owner.

The Data Owner shall coordinate data protection compliance within the department.

9.27 Responsibilities of Data Owners

Departmental Data Owners shall:

a. identify personal data processed by their department;

b. ensure appropriate collection practices;

c. approve access based on operational need;

d. maintain data inventories;

e. review data accuracy;

f. ensure secure storage;

g. monitor compliance with retention requirements;

h. report risks and incidents;

i. support data subject requests; and

j. coordinate with the Data Protection Officer.

PART XIV

RESPONSIBILITIES OF ALL STAFF AND AFFILIATED PERSONNEL

9.28 General Responsibility

Every person working with or representing ILA has a personal responsibility to protect personal data.

This applies to:

- employees;
- volunteers;
- interns;
- consultants;
- temporary staff;
- board members;
- contractors; and
- partner personnel accessing ILA information.

9.29 Staff Obligations

All personnel shall:

a. comply with this Policy;

b. maintain confidentiality;

c. access information only for authorized purposes;

d. protect passwords and credentials;

e. secure physical and electronic records;

f. report suspected breaches;

g. complete required training;

h. follow approved procedures;

i. avoid unauthorized disclosure; and

j. cooperate with investigations.

PART XV

VOLUNTEERS, INTERNS AND CONSULTANTS

9.30 Extended Personnel Obligations

Volunteers, interns, consultants, and other non-employees who access ILA information shall comply with the same data protection standards applicable to employees.

9.31 Contractual Requirements

Before accessing personal data, external personnel shall, where appropriate:

a. sign confidentiality agreements;

b. receive relevant instructions;

c. receive appropriate access permissions;

d. understand reporting obligations;

e. comply with security requirements; and

f. return or destroy information upon completion of engagement.

PART XVI

PARTNER AND THIRD-PARTY RESPONSIBILITIES

9.32 Responsibilities of Partners

Organizations partnering with ILA shall ensure that personal data received from or shared with ILA is handled responsibly.

9.33 Partner Obligations

Partners shall:

a. use information only for agreed purposes;

b. maintain confidentiality;

c. implement appropriate safeguards;

d. restrict access;

e. report incidents;

f. comply with agreements;

g. prevent unauthorized disclosure; and

h. support compliance monitoring.

PART XVII

DATA PROTECTION COMMITTEE

9.34 Establishment of Data Protection Committee

ILA may establish a Data Protection Committee to provide coordinated oversight of privacy and information security matters.

9.35 Composition of Committee

The Committee may include representatives from:

a. Executive Management;

b. Legal Department;

c. Data Protection Function;

d. ICT Unit;

e. HR Department;

f. MEAL Unit;

g. Safeguarding Unit;

h. Finance and Administration; and

i. Programme Departments.

9.36 Responsibilities of Data Protection Committee

The Committee may:

a. review significant privacy risks;

b. monitor implementation of this Policy;

c. review major incidents;

d. advise on high-risk processing;

e. support organizational awareness;

f. review compliance reports;

g. recommend improvements; and

h. promote organizational accountability.

PART XVIII

REPORTING STRUCTURES

9.37 Data Protection Reporting

The Data Protection Officer shall provide periodic reports to management regarding:

a. compliance status;

b. data protection risks;

c. incidents;

d. training activities;

e. data subject requests;

f. audit findings;

g. improvement actions; and

h. emerging risks.

9.38 Significant Matters

Serious matters shall be escalated to senior management and, where appropriate, the Board.

These may include:

a. major data breaches;

b. significant confidentiality failures;

c. repeated compliance failures;

d. serious safeguarding information risks;

e. legal or regulatory concerns; and

f. substantial security threats.

PART XIX

GOVERNANCE REVIEW AND CONTINUOUS IMPROVEMENT

9.39 Periodic Governance Review

ILA shall periodically review its data protection governance arrangements to ensure they remain effective.

Reviews shall consider:

a. organizational changes;

b. programme expansion;

c. technological developments;

d. legal developments;

e. audit findings;

f. incident lessons;

g. donor expectations; and

h. emerging privacy risks.

9.40 Continuous Improvement

ILA shall continuously strengthen its data protection framework through:

a. policy updates;

b. staff training;

c. improved procedures;

d. technological improvements;

e. risk assessments;

f. stakeholder feedback; and

g. lessons learned.

CHAPTER TEN

DATA PROTECTION COMPLIANCE, AUDIT AND MONITORING

10.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that effective data protection requires continuous monitoring, evaluation, review, and improvement.

Adoption of policies alone is insufficient; ILA shall establish systems to verify that personal data is handled responsibly throughout its lifecycle.

This Chapter establishes the framework for:

a. compliance monitoring;

b. internal and external audits;

c. risk reviews;

d. security assessments;

e. reporting mechanisms;

f. corrective actions;

g. accountability measures; and

h. continuous improvement.

PART I

DATA PROTECTION COMPLIANCE FRAMEWORK

10.2 Compliance Commitment

ILA shall maintain a culture of compliance by ensuring that:

a. personal data processing follows approved procedures;

b. staff understand their responsibilities;

c. safeguards are implemented effectively;

d. risks are regularly assessed;

e. incidents are addressed promptly;

f. records are maintained accurately; and

g. improvements are continuously implemented.

10.3 Compliance Principles

ILA's compliance framework shall be guided by:

(a) Accountability

ILA shall demonstrate responsibility for protecting personal data.

(b) Transparency

Information handling practices shall be documented and communicated appropriately.

(c) Risk-Based Approach

Compliance efforts shall prioritize areas presenting the greatest risks.

(d) Continuous Improvement

Processes shall be strengthened based on experience, audits, and lessons learned.

(e) Independent Review

Where appropriate, compliance shall be reviewed objectively.

PART II

DATA PROTECTION COMPLIANCE MONITORING

10.4 Purpose of Monitoring

Data protection monitoring shall ensure that:

a. this Policy is implemented;

b. procedures are followed;

c. security measures remain effective;

d. risks are identified;

e. staff comply with obligations;

f. weaknesses are corrected; and

g. accountability is maintained.

10.5 Monitoring Activities

ILA may conduct monitoring through:

a. compliance reviews;

b. departmental assessments;

c. access reviews;

d. records inspections;

e. system monitoring;

f. staff consultations;

g. training assessments;

h. incident reviews;

i. documentation reviews; and

j. stakeholder feedback.

10.6 Departmental Compliance Reviews

Each department shall periodically review its own compliance with this Policy.

Reviews shall assess:

a. personal data processed;

b. storage arrangements;

c. access controls;

d. information sharing;

e. retention practices;

f. staff awareness;

g. security risks; and

h. outstanding corrective actions.

PART III

DATA PROTECTION AUDITS

10.7 Purpose of Audits

Audits shall provide an independent assessment of whether ILA's data protection practices are effective and compliant.

Audits may evaluate:

a. policy implementation;

b. legal compliance;

c. information security;

d. confidentiality practices;

e. records management;

f. access controls;

g. incident management;

h. third-party compliance; and

i. staff awareness.

10.8 Types of Audits

ILA may undertake:

(a) Internal Audits

Conducted by authorized internal personnel to assess compliance and identify improvements.

(b) ICT Security Audits

Focused on technical safeguards, systems, networks, and cybersecurity controls.

(c) External Audits

Conducted by independent auditors, consultants, donors, or competent reviewers where required.

(d) Programme Compliance Reviews

Focused on data practices within specific projects or activities.

10.9 Audit Frequency

Audit frequency shall be determined based on:

a. level of risk;

b. sensitivity of information;

c. previous findings;

d. organizational changes;

e. donor requirements;

f. incidents experienced; and

g. available resources.

PART IV

AUDIT PROCESS

10.10 Audit Planning

Before an audit, ILA shall define:

a. scope;

b. objectives;

c. methodology;

d. responsible auditors;

e. departments involved;

f. timeframe; and

g. reporting arrangements.

10.11 Audit Evidence

Audits may examine:

a. policies and procedures;

b. contracts;

c. records;

d. access logs;

e. databases;

f. training records;

g. incident reports;

h. retention schedules;

i. security controls; and

j. interviews with personnel.

10.12 Audit Findings Classification

Findings may be classified as:

Critical

Issues creating significant risk of harm, legal exposure, or serious confidentiality failure.

Major

Important weaknesses requiring timely corrective action.

Moderate

Issues requiring improvement but presenting limited immediate risk.

Minor

Administrative or procedural improvements.

PART V

CORRECTIVE ACTION AND IMPROVEMENT

10.13 Corrective Action Plans

Where compliance weaknesses are identified, ILA shall develop corrective action plans.

Plans shall include:

a. identified issue;

b. required action;

c. responsible officer;

d. completion deadline;

e. required resources;

f. monitoring arrangements; and

g. completion status.

10.14 Priority of Corrective Actions

Priority shall be given to matters involving:

a. sensitive personal information;

b. vulnerable individuals;

c. safeguarding concerns;

d. legal privilege;

e. significant security weaknesses;

f. repeated non-compliance;

g. potential legal violations.

10.15 Follow-Up Reviews

ILA shall conduct follow-up reviews to confirm that corrective actions have been implemented.

Where actions remain incomplete, management shall determine further measures.

PART VI

COMPLIANCE REPORTING

10.16 Data Protection Reports

The Data Protection Officer shall prepare periodic reports addressing:

a. compliance status;

b. audit findings;

c. incidents;

d. risks;

e. training activities;

f. data subject requests;

g. corrective actions;

h. improvement recommendations.

10.17 Management Reporting

Reports shall be submitted to appropriate management structures, including:

a. Executive Director;

b. Data Protection Committee;

c. Board of Directors where appropriate.

10.18 Serious Compliance Issues

Significant matters shall be escalated without delay where they involve:

a. major breaches;

b. serious confidentiality failures;

c. safeguarding information risks;

d. legal exposure;

e. donor compliance concerns;

f. repeated failures; or

g. significant security threats.

PART VII

DATA PROTECTION PERFORMANCE INDICATORS

10.19 Compliance Indicators

ILA may monitor performance through indicators such as:

a. percentage of staff trained;

b. number of data breaches reported;

c. number of privacy assessments completed;

d. completion rate of corrective actions;

e. number of access reviews conducted;

f. percentage of departments reviewed;

g. response time to incidents;

h. compliance with retention schedules; and

i. number of unresolved privacy risks.

10.20 Use of Performance Information

Performance information shall be used to:

a. identify weaknesses;

b. allocate resources;

c. improve procedures;

d. strengthen accountability;

e. inform management decisions; and

f. enhance organizational learning.

PART VIII

STAFF COMPLIANCE MONITORING

10.21 Purpose of Staff Compliance Monitoring

ILA recognizes that effective data protection depends significantly on the conduct and awareness of individuals handling personal data.

The Organization shall monitor staff compliance to ensure that personnel:

a. understand their responsibilities;

b. follow approved procedures;

c. maintain confidentiality;

d. complete required training;

e. report incidents appropriately; and

f. apply security practices consistently.

10.22 Methods of Staff Compliance Monitoring

Staff compliance may be monitored through:

a. training attendance records;

b. confidentiality agreements;

c. performance reviews;

d. supervisory checks;

e. access reviews;

f. disciplinary records;

g. incident reports;

h. staff interviews; and

i. compliance assessments.

10.23 Performance Management Integration

Data protection responsibilities may be incorporated into:

a. job descriptions;

b. employment agreements;

c. performance objectives;

d. staff assessments; and

e. professional development plans.

PART IX

TRAINING COMPLIANCE MONITORING

10.24 Training Requirements

ILA shall maintain records of data protection training provided to:

- employees;
- volunteers;
- interns;
- consultants;
- contractors;
- Board members; and
- relevant partners.

10.25 Training Monitoring

The Data Protection Officer and Human Resources Department shall monitor:

a. completion rates;

b. training effectiveness;

c. staff understanding;

d. areas requiring additional support; and

e. emerging training needs.

10.26 Additional Training Requirements

Additional training may be required where:

a. staff handle sensitive information;

b. new systems are introduced;

c. incidents occur;

d. compliance failures are identified;

e. staff responsibilities change; or

f. new legal obligations arise.

PART X

THIRD-PARTY COMPLIANCE MONITORING

10.27 Monitoring Third Parties

Where external parties process ILA personal data, the Organization shall monitor compliance with agreed privacy and security requirements.

Third parties include:

a. consultants;

b. contractors;

c. technology providers;

d. service providers;

e. research partners;

f. implementing partners; and

g. donor-funded project partners.

10.28 Third-Party Compliance Measures

Monitoring may include:

a. review of contractual obligations;

b. security questionnaires;

c. compliance reports;

d. audits;

e. confidentiality confirmations;

f. incident reporting reviews;

g. access reviews; and

h. performance assessments.

10.29 Third-Party Non-Compliance

Where a third party fails to comply with data protection requirements, ILA may:

a. require corrective action;

b. restrict access;

c. suspend information sharing;

d. require additional safeguards;

e. terminate arrangements; or

f. pursue contractual remedies.

PART XI

DONOR AND PARTNER COMPLIANCE REQUIREMENTS

10.30 Donor Compliance

Where donor agreements impose data protection requirements, ILA shall ensure that:

a. obligations are identified;

b. responsible persons are assigned;

c. compliance is documented;

d. reporting requirements are fulfilled; and

e. donor assessments are supported.

10.31 Partner Compliance Reviews

For programmes implemented jointly with partners, ILA shall assess:

a. partner data handling practices;

b. confidentiality arrangements;

c. security safeguards;

d. information-sharing procedures;

e. incident management capacity; and

f. compliance with agreed standards.

PART XII

RECORDS OF PROCESSING ACTIVITIES

10.32 Establishment of Processing Records

ILA shall maintain records of significant personal data processing activities to support accountability and transparency.

10.33 Contents of Processing Records

Records may include:

a. department responsible;

b. purpose of processing;

c. categories of personal data;

d. categories of individuals affected;

e. sources of information;

f. recipients of information;

g. storage arrangements;

h. retention periods;

i. security measures; and

j. responsible officers.

10.34 Review of Processing Records

Processing records shall be reviewed periodically and updated when:

a. new programmes begin;

b. systems change;

c. new categories of data are collected;

d. partnerships change;

e. risks change; or

f. processing activities end.

PART XIII

DATA PROTECTION COMPLIANCE REGISTER

10.35 Establishment of Compliance Register

ILA shall maintain a Data Protection Compliance Register to record key compliance activities.

13.36 Contents of Compliance Register

The register may include:

a. completed Privacy Impact Assessments;

b. training records;

c. audits conducted;

d. incidents recorded;

e. corrective actions;

f. data-sharing agreements;

g. processing records;

h. retention reviews;

i. access reviews; and

j. policy reviews.

10.37 Purpose of Compliance Register

The Compliance Register shall support:

a. accountability;

b. institutional memory;

c. audit preparation;

d. donor reporting;

e. risk management; and

f. continuous improvement.

PART XIV

MANAGEMENT REVIEW OF DATA PROTECTION FRAMEWORK

10.38 Management Review

ILA management shall periodically review the effectiveness of the data protection framework.

10.39 Matters for Review

Management review shall consider:

a. audit findings;

b. breach incidents;

c. compliance performance;

d. risk assessments;

e. training effectiveness;

f. technological developments;

g. resource requirements;

h. legal developments;

i. stakeholder feedback; and

j. improvement opportunities.

10.40 Outcomes of Management Review

Management review may result in:

a. policy amendments;

b. new procedures;

c. additional resources;

d. enhanced controls;

e. revised training programmes;

f. system improvements; and

g. organizational changes.

PART XV

CONTINUOUS IMPROVEMENT FRAMEWORK

10.41 Commitment to Improvement

ILA shall continuously improve its data protection practices through:

a. monitoring;

b. evaluation;

c. audits;

d. incident learning;

e. stakeholder feedback;

f. technological improvements;

g. staff development; and

h. updated procedures.

10.42 Lessons Learned

ILA shall use lessons from:

- data breaches;
- audits;
- assessments;
- complaints;
- reviews;
- programme implementation; and
- stakeholder engagement

to strengthen future data protection practices.

10.43 Review of Policy Effectiveness

This Data Protection and Privacy Policy shall be reviewed periodically to ensure that it remains:

a. effective;

b. relevant;

c. practical;

d. aligned with organizational needs;

e. consistent with legal requirements; and

f. responsive to emerging risks.

CHAPTER ELEVEN

DATA PROTECTION TRAINING, AWARENESS AND ORGANIZATIONAL CULTURE

11.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that effective data protection requires informed, responsible, and accountable personnel.

Technology and procedures alone cannot guarantee privacy protection. Staff members, volunteers, consultants, partners, and other persons handling personal data must understand:

a. their responsibilities;

b. confidentiality obligations;

c. risks associated with misuse of information;

d. procedures for protecting personal data;

e. incident reporting requirements; and

f. the rights of individuals whose information is processed.

ILA shall therefore establish a comprehensive data protection training and awareness programme.

PART I

DATA PROTECTION CULTURE

11.2 Commitment to Privacy Culture

ILA shall promote an organizational culture where:

a. privacy is respected;

b. confidentiality is valued;

c. information is handled responsibly;

d. risks are reported promptly;

e. individuals are treated with dignity;

f. security practices become routine; and

g. accountability is embedded in daily operations.

11.3 Principles of Organizational Data Protection Culture

ILA shall promote the following principles:

(a) Everyone Has Responsibility

Protection of personal data is the responsibility of every person handling information.

(b) Confidentiality Is Fundamental

Confidentiality is essential to maintaining trust with clients, beneficiaries, partners, and communities.

(c) Prevention Is Better Than Correction

Personnel shall identify and prevent risks before harm occurs.

(d) Reporting Is Encouraged

Staff shall report mistakes, risks, and incidents without fear of retaliation.

(e) Continuous Learning

Data protection knowledge shall be continuously strengthened.

PART II

TRAINING REQUIREMENTS

11.4 Mandatory Training

ILA shall require all personnel who process personal data to complete appropriate data protection training.

This shall apply to:

a. employees;

b. Board members;

c. volunteers;

d. interns;

e. consultants;

f. contractors;

g. temporary staff; and

h. relevant partner personnel.

11.5 Timing of Training

Training shall be provided:

a. during induction;

b. before access to sensitive information is granted;

c. periodically through refresher sessions;

d. when significant policy changes occur;

e. when new systems are introduced; and

f. following incidents or identified weaknesses.

PART III

STAFF INDUCTION TRAINING

11.6 Data Protection Induction

All new personnel shall receive basic data protection orientation before handling personal information.

11.7 Induction Topics

Training shall cover:

a. principles of data protection;

b. confidentiality obligations;

c. types of personal data;

d. sensitive information handling;

e. information security practices;

f. access control responsibilities;

g. reporting procedures;

h. client confidentiality;

i. safeguarding confidentiality; and

j. consequences of non-compliance.

PART IV

SPECIALIZED TRAINING PROGRAMMES

11.8 Legal Staff Training

Legal personnel shall receive additional training on:

a. lawyer-client confidentiality;

b. legal privilege;

c. secure case management;

d. evidence protection;

e. witness information;

f. court disclosure requirements; and

g. ethical obligations.

11.9 Safeguarding Personnel Training

Personnel handling safeguarding matters shall receive training on:

a. survivor confidentiality;

b. sensitive information management;

c. informed consent;

d. referral confidentiality;

e. safe information sharing;

f. protection against retaliation; and

g. safeguarding reporting systems.

11.10 ICT Personnel Training

ICT personnel shall receive specialized training on:

a. cybersecurity;

b. access management;

c. system security;

d. encryption;

e. vulnerability management;

f. incident response;

g. backup protection; and

h. secure system administration.

11.11 MEAL and Research Personnel Training

Personnel involved in monitoring, evaluation, research, or data collection shall receive training on:

a. responsible data collection;

b. informed consent;

c. anonymization;

d. secure storage;

e. participant protection;

f. data quality;

g. ethical research practices; and

h. reporting obligations.

11.12 Finance and HR Personnel Training

Finance and HR personnel shall receive training on:

a. employee confidentiality;

b. payroll information protection;

c. personnel records management;

d. secure document handling;

e. access restrictions; and

f. information retention.

PART V

AWARENESS PROGRAMMES

11.13 Awareness Activities

ILA shall conduct ongoing awareness activities through:

a. workshops;

b. staff meetings;

c. newsletters;

d. email reminders;

e. posters;

f. guidance notes;

g. security alerts;

h. practical exercises; and

i. awareness campaigns.

11.14 Key Awareness Messages

Awareness activities shall reinforce:

a. confidentiality obligations;

b. secure password practices;

c. safe handling of documents;

d. risks of unauthorized sharing;

e. phishing awareness;

f. incident reporting;

g. responsible use of technology; and

h. protection of vulnerable persons.

PART VI

CONFIDENTIALITY COMMITMENTS

11.15 Confidentiality Agreements

Personnel handling personal data may be required to sign confidentiality commitments confirming:

a. understanding of obligations;

b. commitment to protect information;

c. prohibition against unauthorized disclosure;

d. responsibility after leaving ILA; and

e. acceptance of accountability measures.

11.16 Continuing Confidentiality Obligations

Confidentiality obligations shall continue after:

a. employment ends;

b. consultancy concludes;

c. volunteering ends;

d. partnership terminates; or

e. access permissions are removed.

PART VII

TRAINING ASSESSMENT AND EFFECTIVENESS

11.17 Evaluation of Training

ILA shall assess whether training has achieved its objectives through:

a. knowledge assessments;

b. feedback surveys;

c. practical exercises;

d. compliance reviews;

e. incident analysis; and

f. supervisory observations.

11.18 Improving Training Programmes

Training programmes shall be updated based on:

a. assessment results;

b. audit findings;

c. new risks;

d. technological developments;

e. legal changes;

f. staff feedback; and

g. organizational learning.

PART VIII

TRAINING RECORD MANAGEMENT

11.19 Training Records

ILA shall maintain records of data protection training, including:

a. participant names;

b. training dates;

c. training topics;

d. trainers;

e. attendance records;

f. assessment results; and

g. refresher requirements.

11.20 Monitoring Training Compliance

The Human Resources Department and Data Protection Officer shall monitor:

a. completion rates;

b. overdue training;

c. departmental compliance;

d. staff competency; and

e. additional training needs.

PART IX

PARTNER, CONTRACTOR AND THIRD-PARTY AWARENESS

11.21 Awareness Requirements for External Persons

ILA recognizes that external persons who access personal data may create privacy risks if they lack adequate understanding of confidentiality obligations.

Accordingly, ILA shall ensure that relevant external persons receive appropriate awareness and guidance before accessing organizational information.

This applies to:

a. implementing partners;

b. consultants;

c. contractors;

d. researchers;

e. service providers;

f. volunteers; and

g. temporary personnel.

11.22 External Awareness Measures

ILA may provide external persons with:

a. confidentiality requirements;

b. data protection guidelines;

c. contractual obligations;

d. security instructions;

e. reporting procedures;

f. safeguarding requirements; and

g. restrictions on information use.

11.23 Partner Compliance Confirmation

Where appropriate, partners and contractors shall confirm that they:

a. understand data protection obligations;

b. maintain confidentiality;

c. apply appropriate safeguards;

d. report incidents;

e. comply with agreements; and

f. cooperate with compliance reviews.

PART X

BOARD AND GOVERNANCE AWARENESS

11.24 Board Data Protection Awareness

The Board of Directors shall receive appropriate awareness regarding:

a. institutional privacy responsibilities;

b. governance obligations;

c. significant data protection risks;

d. major incidents;

e. compliance performance;

f. resource requirements; and

g. strategic improvements.

11.25 Executive Management Awareness

Senior management shall understand:

a. their accountability obligations;

b. organizational risks;

c. compliance responsibilities;

d. incident response duties;

e. policy implementation requirements; and

f. the importance of privacy culture.

PART XI

DATA PROTECTION CHAMPIONS

11.26 Establishment of Data Protection Champions

ILA may designate Data Protection Champions within departments to support implementation of this Policy.

11.27 Role of Data Protection Champions

Data Protection Champions shall:

a. promote privacy awareness;

b. support staff understanding;

c. identify departmental risks;

d. encourage good practices;

e. support compliance monitoring;

f. communicate updates; and

g. coordinate with the Data Protection Officer.

11.28 Selection of Champions

Champions should be persons who:

a. understand departmental operations;

b. handle information responsibly;

c. demonstrate commitment to confidentiality;

d. communicate effectively; and

e. cooperate with compliance activities.

PART XII

PRIVACY COMMUNICATION STRATEGY

11.29 Purpose of Communication

ILA shall maintain effective communication mechanisms to ensure that privacy expectations are understood throughout the organization.

11.30 Communication Channels

Privacy information may be communicated through:

a. staff meetings;

b. internal notices;

c. email communications;

d. training sessions;

e. policy updates;

f. guidance documents;

g. digital platforms; and

h. awareness campaigns.

11.31 Communication Topics

Communications may address:

a. policy changes;

b. emerging privacy risks;

c. security alerts;

d. lessons from incidents;

e. good practices;

f. new technologies;

g. legal developments; and

h. organizational expectations.

PART XIII

TRAINING RESPONSIBILITIES

11.32 Role of Human Resources Department

The Human Resources Department shall:

a. coordinate staff training arrangements;

b. maintain training records;

c. include privacy obligations in induction;

d. monitor completion;

e. support disciplinary processes where required; and

f. coordinate refresher programmes.

11.33 Role of Data Protection Officer

The Data Protection Officer shall:

a. develop training content;

b. advise on training needs;

c. conduct or coordinate training;

d. evaluate effectiveness;

e. provide technical guidance;

f. monitor compliance; and

g. recommend improvements.

11.34 Role of Department Heads

Department Heads shall:

a. ensure staff participation;

b. identify training needs;

c. reinforce compliance;

d. monitor application of learning;

e. address weaknesses; and

f. promote responsible information handling.

PART XIV

NON-COMPLIANCE WITH TRAINING REQUIREMENTS

11.35 Failure to Complete Required Training

Where personnel fail to complete mandatory data protection training, ILA may:

a. restrict access to personal information;

b. require completion before restoring access;

c. provide additional guidance;

d. address the matter through supervision;

e. apply disciplinary procedures where appropriate.

11.36 Unauthorized Access Due to Training Failure

Where failure to complete training contributes to:

a. unauthorized disclosure;

b. misuse of information;

c. security incidents;

d. confidentiality breaches; or

e. harm to individuals,

ILA shall take appropriate corrective measures.

PART XV

CONTINUOUS LEARNING FRAMEWORK

11.37 Commitment to Continuous Learning

ILA shall maintain continuous improvement in data protection knowledge through:

a. regular training;

b. experience sharing;

c. incident reviews;

d. updated guidance;

e. professional development;

f. peer learning; and

g. engagement with relevant standards and best practices.

11.38 Lessons Learned Approach

ILA shall use lessons from:

a. audits;

b. complaints;

c. security incidents;

d. monitoring activities;

e. programme implementation;

f. partner experiences; and

g. emerging technologies

to improve future training and awareness initiatives.

11.39 Annual Training Review

At least annually, ILA shall review its data protection training programme to determine:

a. effectiveness;

b. relevance;

c. coverage;

d. resource needs;

e. emerging risks; and

f. areas requiring improvement.

CHAPTER TWELVE

DATA PROTECTION INCIDENT RESPONSE AND BREACH MANAGEMENT

12.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that despite preventive measures, personal data incidents may occur due to human error, technological failures, unauthorized access, security threats, or other circumstances.

ILA shall maintain an effective incident response framework to ensure that:

a. incidents are identified quickly;

b. risks are assessed promptly;

c. harm is minimized;

d. affected persons are protected;

e. corrective measures are implemented; and

f. lessons are incorporated into future practices.

PART I

DATA PROTECTION INCIDENTS

12.2 Definition of a Data Protection Incident

A data protection incident is any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of personal data.

12.3 Examples of Data Protection Incidents

Incidents may include:

a. unauthorized access to personal data;

b. accidental disclosure of confidential information;

c. loss or theft of files or devices;

d. sending information to the wrong recipient;

e. cyberattacks;

f. malware or ransomware attacks;

g. unauthorized copying of records;

h. improper disposal of documents;

i. alteration or destruction of information;

j. misuse of personal information;

k. loss of client files;

l. inappropriate publication of personal information; or

m. breach of confidentiality obligations.

PART II

INCIDENT RESPONSE PRINCIPLES

12.4 Response Principles

ILA shall manage incidents according to the following principles:

(a) Prompt Action

Incidents shall be reported and addressed without unnecessary delay.

(b) Protection of Individuals

The safety and interests of affected persons shall be prioritized.

(c) Confidential Handling

Incident information shall itself be protected.

(d) Evidence Preservation

Relevant evidence shall be preserved for investigation.

(e) Accountability

Actions taken shall be documented.

(f) Learning and Improvement

Lessons shall be used to strengthen controls.

PART III

INCIDENT IDENTIFICATION AND REPORTING

12.5 Duty to Report Incidents

All personnel who become aware of a suspected data protection incident shall report it immediately.

This obligation applies to:

a. employees;

b. volunteers;

c. interns;

d. consultants;

e. contractors;

f. partners; and

g. service providers.

12.6 Reporting Channels

Incidents may be reported through:

a. Data Protection Officer;

b. ICT Unit;

c. Department Head;

d. Legal Department;

e. Safeguarding Officer where applicable;

f. management reporting channels; or

g. designated incident reporting mechanisms.

12.7 Information Required in Incident Reports

Where possible, reports should include:

a. date and time of incident;

b. location;

c. persons involved;

d. type of information affected;

e. suspected cause;

f. persons who may be affected;

g. immediate actions taken; and

h. additional concerns.

PART IV

IMMEDIATE RESPONSE ACTIONS

12.8 Initial Response

Upon receiving a report, ILA shall:

a. acknowledge receipt;

b. record the incident;

c. assess immediate risks;

d. prevent further exposure;

e. secure affected information;

f. preserve evidence;

g. identify responsible persons; and

h. initiate investigation.

12.9 Containment Measures

Containment actions may include:

a. disabling compromised accounts;

b. recovering improperly shared information;

c. restricting access;

d. isolating affected systems;

e. securing physical records;

f. changing passwords;

g. blocking unauthorized users; and

h. suspending risky activities.

PART V

INCIDENT CLASSIFICATION

12.10 Purpose of Classification

ILA shall classify incidents according to seriousness to determine appropriate response measures.

12.11 Incident Categories

Incidents may be classified as:

Level One: Minor Incident

Limited impact with minimal risk to individuals.

Examples:

- administrative errors;
- isolated mistakes;
- minor access issues.

Level Two: Moderate Incident

An incident involving increased risk requiring corrective action.

Examples:

- unauthorized access;
- disclosure of limited personal information;
- repeated procedural failures.

Level Three: Serious Incident

An incident involving significant risk to individuals.

Examples:

- exposure of sensitive client information;
- loss of confidential files;
- unauthorized disclosure of safeguarding information.

Level Four: Critical Incident

A major breach creating serious risk to individuals, including:

- mass disclosure;
- exposure of survivor information;
- compromise of legal case files;
- threats to personal safety;
- significant cyberattacks.

PART VI

INCIDENT INVESTIGATION

12.12 Investigation Process

ILA shall investigate incidents to determine:

a. what happened;

b. when it occurred;

c. how it occurred;

d. information affected;

e. persons affected;

f. level of harm;

g. responsible factors;

h. corrective actions required.

12.13 Investigation Team

Depending on the incident, the investigation may involve:

a. Data Protection Officer;

b. ICT Officer;

c. Legal Department;

d. Safeguarding Officer;

e. Human Resources;

f. relevant Department Head;

g. external specialists where necessary.

12.14 Investigation Confidentiality

Incident investigations shall be conducted confidentially.

Information shall only be shared with persons who require it for legitimate response purposes.

PART VII

BREACH RISK ASSESSMENT

12.15 Assessment Factors

ILA shall assess:

a. type of information affected;

b. sensitivity of information;

c. number of individuals affected;

d. vulnerability of affected persons;

e. likelihood of misuse;

f. possible consequences;

g. security measures in place; and

h. actions already taken.

12.16 Special Considerations

Enhanced assessment shall apply where incidents involve:

- children;
- survivors of violence;
- legal aid clients;
- witnesses;
- confidential legal information;
- health information;
- human rights documentation; or
- security-sensitive information.

PART VIII

DATA BREACH NOTIFICATION PROCEDURES

12.17 Purpose of Notification

ILA shall ensure appropriate notification of data protection incidents where necessary to protect affected individuals, comply with obligations, and support accountability.

Notification decisions shall consider:

a. seriousness of the incident;

b. risk to affected persons;

c. sensitivity of information involved;

d. likelihood of harm;

e. legal and contractual obligations; and

f. safeguarding considerations.

12.18 Internal Notification

Serious or significant incidents shall be reported internally to appropriate authorities, including:

a. Data Protection Officer;

b. Executive Director;

c. Legal Department;

d. ICT Unit;

e. Safeguarding Officer where relevant;

f. Department Head concerned; and

g. Board of Directors where appropriate.

12.19 External Notification

Where required or appropriate, ILA may notify:

a. affected individuals;

b. relevant authorities;

c. donors;

d. contractual partners;

e. service providers;

f. affected communities; or

g. other stakeholders.

PART IX

COMMUNICATION WITH AFFECTED PERSONS

12.20 Notification Principles

Where affected persons need to be informed, communication shall be:

a. timely;

b. clear;

c. accurate;

d. sensitive;

e. accessible; and

f. appropriate to the circumstances.

12.21 Content of Notifications

A notification may include:

a. description of the incident;

b. type of information affected;

c. possible risks;

d. actions taken by ILA;

e. steps individuals may take to protect themselves;

f. available support mechanisms; and

g. contact information for further assistance.

12.22 Protection-Sensitive Communication

Where notification may increase risks to individuals, especially:

- survivors;
- witnesses;
- legal aid clients;
- children;
- vulnerable persons; or
- persons facing threats,

ILA shall carefully assess the safest communication approach.

PART X

CORRECTIVE AND REMEDIAL MEASURES

12.23 Immediate Remedial Actions

Following an incident, ILA may implement measures including:

a. securing systems;

b. recovering information;

c. correcting errors;

d. restricting access;

e. providing assistance to affected persons;

f. strengthening controls;

g. updating procedures; and

h. conducting additional training.

12.24 Long-Term Corrective Actions

Corrective measures may include:

a. system improvements;

b. policy amendments;

c. improved supervision;

d. enhanced security measures;

e. revised agreements;

f. additional risk assessments;

g. disciplinary action where appropriate; and

h. organizational learning activities.

PART XI

ROOT CAUSE ANALYSIS

12.25 Purpose of Root Cause Analysis

ILA shall conduct root cause analysis for significant incidents to determine underlying causes and prevent recurrence.

12.26 Areas of Analysis

The review shall consider:

a. human factors;

b. system weaknesses;

c. procedural failures;

d. inadequate training;

e. security vulnerabilities;

f. third-party failures;

g. management oversight; and

h. resource limitations.

12.27 Root Cause Report

A root cause report may include:

a. incident summary;

b. timeline of events;

c. contributing factors;

d. identified weaknesses;

e. corrective measures;

f. responsible persons; and

g. implementation deadlines.

PART XII

POST-INCIDENT REVIEW AND LESSONS LEARNED

12.28 Post-Incident Review

After resolution of a significant incident, ILA shall conduct a review to evaluate:

a. effectiveness of response;

b. adequacy of procedures;

c. communication effectiveness;

d. remaining risks;

e. improvement opportunities; and

f. lessons learned.

12.29 Lessons Learned Integration

Lessons learned shall be incorporated into:

a. policies;

b. procedures;

c. training programmes;

d. risk assessments;

e. security controls;

f. programme planning; and

g. future decision-making.

PART XIII

DATA BREACH REGISTER

12.30 Establishment of Breach Register

ILA shall maintain a Data Breach Register recording significant personal data incidents.

12.31 Contents of Breach Register

The register shall include:

a. incident reference number;

b. date of incident;

c. date reported;

d. nature of breach;

e. information affected;

f. individuals affected;

g. risk assessment;

h. actions taken;

i. notification decisions;

j. corrective measures;

k. responsible officers; and

l. closure date.

12.32 Purpose of Breach Register

The register shall support:

a. accountability;

b. audit requirements;

c. trend analysis;

d. prevention of recurrence;

e. management reporting; and

f. organizational learning.

PART XIV

RESPONSIBILITIES FOR INCIDENT MANAGEMENT

12.33 Responsibilities of All Personnel

All personnel shall:

a. report suspected incidents;

b. protect evidence;

c. cooperate with investigations;

d. maintain confidentiality;

e. follow response instructions; and

f. implement corrective actions assigned.

12.34 Responsibilities of Data Protection Officer

The DPO shall:

a. coordinate incident response;

b. maintain incident records;

c. advise management;

d. assess notification requirements;

e. monitor corrective actions;

f. support investigations; and

g. prepare incident reports.

12.35 Responsibilities of ICT Unit

The ICT Unit shall:

a. contain technical incidents;

b. secure affected systems;

c. investigate cybersecurity issues;

d. preserve technical evidence;

e. restore systems;

f. improve security controls; and

g. provide technical reports.

12.36 Responsibilities of Legal Department

The Legal Department shall:

a. assess legal obligations;

b. advise on disclosure;

c. protect confidentiality;

d. assess liability risks;

e. review notifications;

f. advise on contractual implications; and

g. support dispute management.

12.37 Responsibilities of Safeguarding Unit

Where safeguarding information is affected, the Safeguarding Unit shall:

a. assess risks to affected persons;

b. ensure survivor-centred responses;

c. advise on safe communication;

d. coordinate protection measures; and

e. prevent further harm.

PART XV

ANNEX: DATA BREACH INCIDENT REPORT TEMPLATE

12.38 Incident Report Structure

ILA shall maintain a standard Data Breach Incident Report containing:

Section One: Incident Details

- Incident reference number;
- Date and time;
- Location;
- Reporting person;

- Department involved.

Section Two: Description of Incident

- What happened;
- How it occurred;
- Information affected;
- Systems or records involved.

Section Three: Risk Assessment

- Persons affected;
- Sensitivity of information;
- Potential harm;
- Risk level.

Section Four: Response Actions

- Immediate containment;
- Investigation actions;
- Notifications;
- Corrective measures.

Section Five: Closure Review

- Root cause;
- Lessons learned;
- Preventive actions;
- Responsible persons;
- Completion date.

CHAPTER THIRTEEN

DATA RETENTION, ARCHIVING AND SECURE DISPOSAL

13.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that responsible management of personal data requires not only protecting information during use but also ensuring that information is retained only for appropriate periods and securely disposed of when no longer necessary.

ILA shall maintain records in a manner that ensures:

a. compliance with legal and contractual obligations;

b. protection of confidentiality;

c. preservation of institutional knowledge;

d. availability of information required for legitimate purposes;

e. prevention of unnecessary accumulation of personal data; and

f. secure disposal of expired records.

PART I

DATA RETENTION PRINCIPLES

13.2 Retention Principle

ILA shall retain personal data only for as long as:

a. necessary for the purpose for which it was collected;

b. required by law;

c. required by contractual obligations;

d. necessary for legitimate organizational purposes; or

e. necessary for legal claims, audits, or accountability.

13.3 Data Minimization and Retention

ILA shall avoid retaining personal data indefinitely without justification.

Departments shall periodically review records to determine whether information remains necessary.

13.4 Retention Factors

Retention periods shall be determined considering:

a. nature of information;

b. sensitivity of information;

c. purpose of processing;

d. legal requirements;

e. donor obligations;

f. operational needs;

g. safeguarding considerations;

h. risk of harm from continued retention; and

i. historical or institutional value.

PART II

RECORD CATEGORIES AND RETENTION REQUIREMENTS

13.5 Legal Aid and Case Files

ILA legal case records may include:

a. client intake information;

b. legal advice records;

c. case notes;

d. pleadings;

e. evidence;

f. correspondence;

g. court documents;

h. witness information; and

i. case closure records.

13.6 Retention of Legal Files

Legal files shall be retained for a period determined by:

a. applicable legal requirements;

b. professional obligations;

c. limitation periods;

d. possibility of appeals or enforcement;

e. client interests; and

f. organizational requirements.

13.7 Confidentiality of Closed Case Files

Closure of a case does not remove confidentiality obligations.

Closed files shall remain protected and accessible only to authorized persons.

PART III

BENEFICIARY AND PROGRAMME RECORDS

13.8 Programme Records

Programme records may include:

a. beneficiary registration information;

b. assistance records;

c. monitoring information;

d. feedback records;

e. evaluation data;

f. referral information; and

g. programme reports.

13.9 Retention of Beneficiary Information

Beneficiary information shall be retained only where necessary for:

a. programme accountability;

b. donor requirements;

c. evaluation purposes;

d. safeguarding;

e. legal obligations; or

f. legitimate organizational purposes.

13.10 Anonymization of Programme Data

Where information is required for research, reporting, learning, or statistical purposes, ILA shall, where possible:

a. remove identifying information;

b. aggregate information; or

c. anonymize records.

PART IV

SAFEGUARDING RECORDS

13.11 Protection of Safeguarding Information

Safeguarding records require enhanced protection due to their sensitive nature.

Such records may include:

a. allegations;

b. survivor information;

c. investigation records;

d. referral information;

e. protection assessments; and

f. disciplinary records.

13.12 Retention of Safeguarding Records

Safeguarding records shall be retained:

a. only as long as necessary;

b. in accordance with safeguarding obligations;

c. with restricted access;

d. securely stored; and

e. according to approved retention schedules.

13.13 Destruction of Safeguarding Records

Disposal of safeguarding records shall only occur:

a. after authorized review;

b. after confirming no ongoing protection need exists;

c. where legal obligations permit destruction; and

d. using secure disposal methods.

PART V

HUMAN RESOURCES RECORDS

13.14 Employee Records

HR records may include:

a. employment applications;

b. contracts;

c. payroll information;

d. performance records;

e. disciplinary records;

f. training records;

g. leave records; and

h. personnel correspondence.

13.15 Retention of HR Records

HR records shall be retained considering:

a. employment obligations;

b. labour requirements;

c. tax obligations;

d. pension requirements;

e. audit requirements; and

f. organizational needs.

PART VI

FINANCIAL AND PROCUREMENT RECORDS

13.16 Financial Records

Financial records may include:

a. payment records;

b. invoices;

b. payroll information;

c. supplier information;

d. procurement documents;

e. audit records;

f. donor financial records; and

g. transaction documentation.

13.17 Retention of Financial Records

Financial records shall be retained according to:

a. applicable financial regulations;

b. tax requirements;

c. donor agreements;

d. audit requirements; and

e. organizational policies

PART VII

DIGITAL ARCHIVING

13.18 Digital Archives

ILA may maintain digital archives to preserve important organizational records.

Digital archives shall be managed to ensure:

a. authenticity;

b. integrity;

c. availability;

d. confidentiality;

e. controlled access; and

f. appropriate backup.

13.19 Digital Archive Controls

Digital archives shall include:

a. access restrictions;

b. authentication controls;

c. encryption where appropriate;

d. backup arrangements;

e. audit logs where available;

f. version control; and

g. secure storage locations.

PART VIII

RECORD RETENTION SCHEDULE

13.20 Establishment of Retention Schedule

ILA shall maintain a Data Retention Schedule specifying:

a. category of records;

b. responsible department;

c. retention period;

d. storage location;

e. disposal method; and

f. approval authority.

13.21 Review of Retention Schedule

The retention schedule shall be reviewed periodically to consider:

a. legal changes;

b. operational changes;

c. donor requirements;

d. risks;

e. technology changes; and

f. lessons learned.

PART IX

SECURE DISPOSAL OF PERSONAL DATA

13.22 Purpose of Secure Disposal

ILA shall ensure that personal data which is no longer required is securely destroyed or permanently removed to prevent:

a. unauthorized access;

b. misuse of information;

c. identity risks;

d. confidentiality breaches;

e. unnecessary accumulation of records; and

f. security vulnerabilities.

13.23 Disposal Principles

Disposal of personal data shall be:

a. authorized;

b. documented;

c. secure;

d. irreversible where appropriate;

e. consistent with retention requirements; and

f. conducted in a manner that protects affected individuals.

PART X

PHYSICAL RECORD DESTRUCTION

13.24 Physical Documents

Physical records may include:

a. paper case files;

b. signed forms;

c. contracts;

d. personnel records;

e. financial documents;

f. assessment reports;

g. correspondence; and

h. confidential notes.

13.25 Approved Destruction Methods

Physical records shall be destroyed through methods such as:

a. cross-cut shredding;

b. secure document destruction services;

c. controlled burning where appropriate and lawful;

d. other approved irreversible destruction methods.

13.26 Prohibited Disposal Practices

Personnel shall not:

a. dispose of confidential documents in ordinary waste bins;

b. leave records in public areas;

c. abandon files in unsecured locations;

d. transfer records without authorization; or

e. destroy records subject to legal hold.

PART XI

DIGITAL DATA DELETION

13.27 Digital Records Disposal

Digital records shall be securely deleted when retention requirements expire.

This applies to:

a. electronic files;

b. databases;

c. emails;

d. cloud storage;

c. portable storage devices;

d. system backups; and

e. electronic case management systems.

13.28 Digital Deletion Methods

Digital deletion may include:

a. secure deletion tools;

b. permanent removal procedures;

c. approved data wiping processes;

d. destruction of storage devices;

e. removal from backup systems where appropriate.

13.29 Disposal of ICT Equipment

Before disposal, transfer, or donation of ICT equipment, ILA shall ensure:

a. personal data is removed;

b. storage devices are securely wiped;

c. accounts are removed;

d. access credentials are disabled;

e. equipment status is recorded; and

f. disposal follows ICT asset procedures.

PART XII

DISPOSAL AUTHORIZATION PROCEDURES

13.30 Approval Before Disposal

No official record containing personal data shall be destroyed without authorization.

13.31 Disposal Approval Process

Before disposal, the responsible department shall:

a. confirm retention period has expired;

b. verify no legal hold exists;

c. confirm no ongoing investigation exists;

d. assess continuing organizational need;

e. prepare disposal request; and

f. obtain approval.

13.32 Authorized Approving Officers

Approval may be provided by:

a. Department Head;

b. Records Officer;

c. Data Protection Officer;

d. Legal Department where legally sensitive information is involved; or

e. Executive Director for significant records.

PART XIII

LEGAL HOLD AND PRESERVATION REQUIREMENTS

13.33 Legal Hold

ILA shall suspend disposal of records where information is required for:

a. litigation;

b. investigations;

c. audits;

d. regulatory inquiries;

e. complaints;

f. disciplinary proceedings; or

g. legal claims.

13.34 Management of Legal Holds

The Legal Department shall coordinate legal holds by:

a. identifying affected records;

b. notifying relevant departments;

c. preventing destruction;

d. monitoring compliance; and

e. authorizing release of holds.

PART XIV

DISPOSAL RECORDS AND REGISTERS

13.35 Disposal Register

ILA shall maintain a Data Disposal Register documenting destruction activities.

13.36 Contents of Disposal Register

The register shall include:

a. description of records destroyed;

b. department responsible;

c. date of disposal;

d. retention period completed;

e. disposal method;

f. approving officer;

g. person conducting disposal; and

h. certificate or evidence of destruction where applicable.

13.37 Disposal Evidence

Where appropriate, ILA shall maintain evidence such as:

a. destruction certificates;

b. disposal reports;

c. ICT wiping records;

d. photographs of destruction activities where appropriate; and

e. contractor confirmations.

PART XV

ARCHIVING RESPONSIBILITIES

13.38 Records Management Responsibility

Each department shall manage its records responsibly throughout their lifecycle.

Departments shall:

a. classify records;

b. maintain accurate records;

c. apply retention schedules;

d. protect confidentiality;

e. identify records for archiving;

f. request disposal approval; and

g. maintain disposal documentation.

13.39 Data Protection Officer Responsibilities

The Data Protection Officer shall:

a. provide guidance on retention;

b. review high-risk disposal decisions;

c. monitor compliance;

d. advise on privacy risks;

e. support retention reviews;

f. maintain oversight records; and

g. recommend improvements.

13.40 Legal Department Responsibilities

The Legal Department shall:

a. advise on legal retention requirements;

b. identify documents requiring preservation;

c. manage legal holds;

d. protect privileged materials;

e. review disposal of legal records; and

f. advise on regulatory obligations.

13.41 ICT Department Responsibilities

The ICT Department shall:

a. manage digital deletion processes;

b. maintain secure archives;

c. protect backups;

d. support secure disposal of devices;

e. maintain technical records; and

f. ensure systems comply with retention requirements.

PART XVI

RETENTION AND DISPOSAL REGISTER TEMPLATE

13.42 Data Retention and Disposal Register

ILA shall maintain a register containing:

Record Category	Responsible Department	Retention Period	Storage Location	Disposal Method	Approval Authority
Legal Case Files	Legal Department	As prescribed	Secure Case Archive	Secure destruction/archive	Legal Department
Beneficiary Records	Programme Department	According to programme requirements	Programme Database	Secure deletion/anonymization	Programme Head
Safeguarding Records	Safeguarding Unit	According to safeguarding requirements	Restricted Archive	Controlled destruction	Safeguarding Officer
HR Records	HR Department	According to employment requirements	HR Records System	Secure destruction	HR Manager
Financial Records	Finance Department	According to financial requirements	Finance Archive	Secure destruction	Finance Manager
ICT Records	ICT Department	According to ICT requirements	Digital Archive	Secure deletion	ICT Manager

CHAPTER FOURTEEN

DATA PROTECTION GOVERNANCE STRUCTURE AND RESPONSIBILITIES

14.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that effective data protection requires clear accountability, defined responsibilities, appropriate oversight, and coordinated implementation.

ILA shall establish a governance structure ensuring that:

a. responsibility for personal data protection is clearly assigned;

b. decision-making authority is defined;

c. risks are identified and managed;

d. compliance is monitored;

e. incidents are properly addressed;

f. staff understand their obligations; and

g. continuous improvement is achieved.

PART I

DATA PROTECTION GOVERNANCE PRINCIPLES

14.2 Accountability Principle

ILA shall maintain accountability for personal data processed under its authority.

The Organization shall be able to demonstrate that it:

a. complies with this Policy;

b. protects personal information;

c. applies appropriate safeguards;

d. manages risks responsibly; and

e. respects individual rights.

14.3 Governance Principles

ILA's data protection governance shall be guided by:

(a) Clear Responsibility

Every person handling personal data shall understand their role.

(b) Separation of Duties

Sensitive decisions shall involve appropriate review and oversight.

(c) Risk-Based Management

Resources shall be directed toward areas of highest risk.

(d) Transparency

Data protection activities shall be documented and reviewable.

(e) Continuous Improvement

The framework shall evolve based on experience and changing risks.

PART II

BOARD OF DIRECTORS OVERSIGHT

14.4 Role of the Board

The Board of Directors provides strategic oversight of ILA's data protection responsibilities.

The Board shall ensure that adequate systems, resources, and accountability mechanisms exist to protect personal data.

14.5 Board Responsibilities

The Board shall:

a. approve the Data Protection and Privacy Policy;

b. provide strategic direction;

c. oversee significant privacy risks;

d. receive reports on major incidents;

e. ensure adequate resources are available;

f. promote ethical information management;

g. support organizational accountability; and

h. review significant compliance concerns.

14.6 Board Confidentiality Obligations

Board members shall:

a. protect confidential information;

b. access personal data only where necessary;

c. comply with confidentiality obligations;

d. avoid unauthorized disclosure; and

e. maintain confidentiality after leaving office.

PART III

EXECUTIVE DIRECTOR RESPONSIBILITIES

14.7 Executive Accountability

The Executive Director has overall responsibility for ensuring implementation of this Policy.

14.8 Responsibilities of Executive Director

The Executive Director shall:

a. provide leadership on data protection;

b. ensure implementation of policies and procedures;

c. appoint responsible officers;

d. approve significant compliance measures;

e. ensure adequate resources;

f. support incident response;

g. promote privacy culture;

h. ensure staff accountability; and

i. report significant matters to the Board.

PART IV

DATA PROTECTION OFFICER

14.9 Appointment of Data Protection Officer

ILA shall designate a Data Protection Officer (DPO) or responsible officer to coordinate data protection compliance.

The DPO shall operate with sufficient independence and authority to perform assigned duties effectively.

14.10 Role of Data Protection Officer

The DPO serves as the central coordination point for:

a. privacy compliance;

b. policy implementation;

c. staff guidance;

d. risk management;

e. monitoring;

f. incident response;

g. awareness programmes; and

h. continuous improvement.

14.11 Responsibilities of Data Protection Officer

The DPO shall:

a. monitor compliance with this Policy;

b. advise departments on data protection matters;

c. maintain compliance records;

d. coordinate privacy assessments;

e. support breach investigations;

f. oversee data subject requests;

g. advise on data sharing;

h. coordinate training;

i. review processing activities;

j. maintain reporting mechanisms; and

k. recommend improvements.

PART V

LEGAL DEPARTMENT RESPONSIBILITIES

14.12 Role of Legal Department

The Legal Department shall provide legal guidance on data protection matters, particularly where confidentiality, privilege, litigation, or regulatory obligations arise.

14.13 Legal Department Responsibilities

The Legal Department shall:

a. interpret legal obligations;

b. advise on confidentiality requirements;

c. protect lawyer-client privilege;

d. review data-sharing agreements;

e. advise on disclosure requests;

f. manage legal holds;

g. support incident investigations;

h. advise on disputes and complaints; and

i. review policy updates.

PART VI

ICT DEPARTMENT RESPONSIBILITIES

14.14 Role of ICT Department

The ICT Department shall ensure that technological systems support secure processing of personal data.

14.15 ICT Responsibilities

The ICT Department shall:

a. implement security controls;

b. manage user access;

c. maintain secure systems;

d. support encryption measures;

e. monitor cybersecurity risks;

f. maintain backups;

g. support incident response;

h. securely dispose of digital records;

i. maintain system documentation; and

j. advise on technology risks.

PART VII

HUMAN RESOURCES DEPARTMENT RESPONSIBILITIES

14.16 Role of HR Department

The Human Resources Department shall ensure that personnel understand and comply with their privacy responsibilities.

14.17 HR Responsibilities

HR shall:

a. include confidentiality obligations in employment documents;

b. coordinate training;

c. maintain employee records securely;

d. manage access changes when staff join or leave;

e. support disciplinary processes;

f. maintain training records;

g. promote ethical conduct; and

h. cooperate with compliance reviews.

PART VIII

PROGRAMME DEPARTMENT RESPONSIBILITIES

14.18 Role of Programme Departments

Programme Departments are responsible for protecting information collected during programme implementation.

14.19 Programme Responsibilities

Departments shall:

a. collect information responsibly;

b. obtain appropriate consent;

c. maintain confidentiality;

d. limit access;

e. protect beneficiary information;

f. follow retention requirements;

g. report incidents;

h. cooperate with monitoring; and

i. ensure partner compliance.

PART IX

MEAL DEPARTMENT RESPONSIBILITIES

14.20 Role of MEAL Unit

The MEAL Unit shall ensure responsible management of monitoring, evaluation, accountability, and learning data.

14.21 MEAL Responsibilities

The MEAL Unit shall:

a. apply ethical data collection methods;

b. protect respondent confidentiality;

c. anonymize information where possible;

d. maintain secure databases;

e. ensure informed participation;

f. manage research-related risks;

g. support accountability mechanisms; and

h. comply with this Policy.

PART X

SAFEGUARDING UNIT RESPONSIBILITIES

14.22 Role of Safeguarding Unit

The Safeguarding Unit shall ensure protection of sensitive safeguarding information.

14.23 Safeguarding Responsibilities

The Safeguarding Unit shall:

a. protect survivor confidentiality;

b. apply survivor-centred approaches;

c. control access to safeguarding records;

d. manage sensitive disclosures;

e. coordinate safe referrals;

f. report serious incidents; and

g. maintain secure records.

PART XI

DEPARTMENTAL DATA OWNERS AND INFORMATION ASSET OWNERS

14.24 Appointment of Data Owners

ILA shall designate responsible persons within departments to oversee specific categories of personal data and information assets.

Data Owners shall ensure that information under their responsibility is managed appropriately throughout its lifecycle.

14.25 Responsibilities of Data Owners

Data Owners shall:

a. understand the information they manage;

b. identify risks associated with processing activities;

c. ensure appropriate access controls;

d. maintain accurate records;

e. implement retention requirements;

f. approve appropriate access requests;

g. monitor compliance within their departments;

h. report risks and incidents; and

i. cooperate with data protection reviews.

14.26 Information Asset Owners

Information Asset Owners shall oversee specific systems, databases, records, or information repositories.

They shall ensure:

a. appropriate security controls;

b. authorized access;

c. proper classification;

d. secure storage;

e. regular review; and

f. responsible disposal.

PART XII

RESPONSIBILITIES OF ALL STAFF AND PERSONNEL

14.27 General Staff Responsibility

Every person working with or accessing ILA information has a responsibility to protect personal data.

14.28 Staff Obligations

All staff members shall:

a. comply with this Policy;

b. protect confidential information;

c. access information only when authorized;

d. use information only for legitimate purposes;

e. maintain secure passwords;

f. avoid unauthorized disclosure;

g. report suspected incidents;

h. complete required training;

i. follow security procedures; and

j. cooperate with investigations.

14.29 Prohibited Staff Conduct

Personnel shall not:

a. access information without authorization;

b. share confidential information improperly;

c. copy records unnecessarily;

d. store information on unauthorized devices;

e. disclose client information;

f. misuse organizational systems;

g. remove confidential records without permission; or

h. destroy records improperly.

PART XIII

VOLUNTEER, INTERN AND CONSULTANT RESPONSIBILITIES

14.30 Application of Policy

This Policy applies equally to:

a. volunteers;

b. interns;

c. consultants;

d. temporary workers;

e. contractors; and

f. project-based personnel.

14.31 Obligations of Non-Employees

Non-employees shall:

a. sign confidentiality commitments where required;

b. complete relevant training;

c. comply with security requirements;

d. protect information accessed during assignments;

e. return or destroy information upon completion; and

f. report incidents immediately.

PART XIV

PARTNER RESPONSIBILITIES

14.32 Partner Accountability

Where ILA shares personal data with partners, those partners shall be required to maintain appropriate protection standards.

14.33 Partner Obligations

Partners shall:

a. process information only for agreed purposes;

b. maintain confidentiality;

c. apply appropriate safeguards;

d. restrict access;

e. report incidents;

f. comply with agreements;

g. cooperate with reviews; and

h. securely dispose of information when required.

PART XV

DATA PROTECTION COMMITTEE

14.34 Establishment of Data Protection Committee

ILA may establish a Data Protection Committee to provide institutional coordination and oversight.

14.35 Composition of Committee

The Committee may include representatives from:

a. Executive Management;

b. Legal Department;

c. Data Protection Officer;

d. ICT Department;

e. Human Resources;

f. Programme Departments;

g. MEAL Unit;

h. Safeguarding Unit; and

i. Finance and Administration.

14.36 Functions of Data Protection Committee

The Committee shall:

a. support implementation of this Policy;

b. review major privacy risks;

c. consider compliance reports;

d. review significant incidents;

e. coordinate improvement initiatives;

f. promote organizational awareness;

g. support cross-department cooperation; and

h. advise senior management.

14.37 Committee Meetings

The Committee shall meet periodically and may convene special meetings where:

a. serious incidents occur;

b. significant risks arise;

c. major systems are introduced;

d. policies require review; or

e. urgent decisions are required.

PART XVI

DATA PROTECTION REPORTING STRUCTURE

14.38 Reporting Lines

Data protection reporting shall follow a structured approach:

Board of Directors

⬇

Executive Director

⬇

Data Protection Officer

⬇

Data Protection Committee

⬇

Department Heads / Data Owners

⬇

Staff, Volunteers, Consultants and Partners

14.39 Regular Reporting

The Data Protection Officer shall provide periodic reports covering:

a. compliance status;

b. training completion;

c. data subject requests;

d. incidents;

e. risk assessments;

f. audits;

g. corrective actions;

h. policy improvements; and

i. emerging risks.

14.40 Serious Matter Reporting

Urgent reporting shall occur where matters involve:

a. serious breaches;

b. safeguarding risks;

c. legal privilege concerns;

d. threats to individuals;

e. significant reputational risks; or

f. major security incidents.

PART XVII

GOVERNANCE REVIEW AND CONTINUOUS IMPROVEMENT

14.41 Periodic Governance Review

ILA shall periodically review its data protection governance structure to ensure that it remains:

a. effective;

b. appropriate;

c. adequately resourced;

d. responsive to risks;

e. aligned with organizational objectives; and

f. consistent with legal and ethical obligations.

14.42 Review Considerations

Governance reviews shall consider:

a. changes in organizational structure;

b. new programmes;

c. technological developments;

d. incident experiences;

e. audit findings;

f. stakeholder feedback;

g. resource requirements; and

h. emerging privacy risks.

14.43 Amendment of Governance Arrangements

Where improvements are required, ILA may:

a. revise responsibilities;

b. establish additional roles;

c. update procedures;

d. strengthen reporting mechanisms;

e. provide additional resources; or

f. amend this Policy.

CHAPTER FIFTEEN

DATA PROTECTION RISK MANAGEMENT AND COMPLIANCE MONITORING

15.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that personal data processing creates potential risks to individuals, programmes, and the Organization.

ILA shall establish a structured risk management framework to:

a. identify privacy risks;

b. assess potential harm;

c. implement appropriate safeguards;

d. monitor compliance;

e. reduce vulnerabilities;

f. strengthen accountability; and

g. promote continuous improvement.

PART I

DATA PROTECTION RISK MANAGEMENT FRAMEWORK

15.2 Purpose of Risk Management

The purpose of data protection risk management is to ensure that:

a. risks are identified before harm occurs;

b. appropriate controls are implemented;

c. sensitive information receives enhanced protection;

d. resources are directed effectively;

e. decisions are evidence-based; and

f. compliance is continuously improved.

15.3 Risk Management Principles

ILA shall manage privacy risks according to the following principles:

(a) Prevention

Risks should be identified and addressed before incidents occur.

(b) Proportionality

Controls shall correspond to the level of risk.

(c) Accountability

Responsible persons shall be assigned for managing risks.

(d) Continuous Monitoring

Risks shall be regularly reviewed.

(e) Documentation

Risk decisions shall be recorded.

PART II

IDENTIFICATION OF DATA PROTECTION RISKS

15.4 Sources of Privacy Risks

ILA shall identify risks arising from:

a. collection of personal information;

b. storage of records;

c. access management;

d. information sharing;

e. technology systems;

f. third-party processing;

g. staff practices;

h. physical security;

i. programme activities;

j. research activities; and

k. organizational changes.

15.5 Categories of Data Protection Risks

Risks may include:

(a) Confidentiality Risks

Unauthorized disclosure or access to information.

Examples:

- leaked client files;
- inappropriate sharing;
- lost documents.

(b) Integrity Risks

Unauthorized alteration or manipulation of information.

Examples:

- incorrect records;
- unauthorized changes;
- compromised databases.

(c) Availability Risks

Loss of access to required information.

Examples:

- system failure;
- ransomware;
- destruction of records.

(d) Compliance Risks

Failure to comply with:

- organizational policies;
- donor obligations;
- professional duties;
- contractual requirements.

(e) Human Rights Risks

Potential harm to individuals resulting from misuse of information.

Examples:

- retaliation;
- discrimination;
- threats;
- loss of protection.

PART III

DATA PROTECTION RISK ASSESSMENT

15.6 Risk Assessment Process

ILA shall conduct risk assessments to determine:

a. likelihood of occurrence;

b. potential impact;

c. affected persons;

d. existing safeguards;

e. remaining risks; and

f. additional controls required.

15.7 Risk Assessment Criteria

Risks shall be assessed based on:

Likelihood

The probability that a risk may occur.

Factors include:

- previous incidents;
- system weaknesses;
- access levels;
- environmental factors.

Impact

The seriousness of possible consequences.

Factors include:

- sensitivity of information;
- number of persons affected;
- vulnerability of individuals;
- potential harm.

15.8 Risk Ratings

ILA may classify risks as:

Low Risk

Limited impact requiring routine controls.

Medium Risk

Requires additional safeguards and monitoring.

High Risk

Requires management attention and corrective action.

Critical Risk

Requires immediate intervention and escalation.

PART IV

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

15.9 Purpose of DPIA

A Data Protection Impact Assessment (DPIA) is a structured assessment used to identify and address privacy risks before undertaking high-risk processing activities.

15.10 Situations Requiring DPIA

ILA shall consider conducting a DPIA where processing involves:

a. sensitive personal information;

b. large-scale data collection;

c. vulnerable groups;

d. new technology systems;

e. systematic monitoring;

f. biometric information;

g. significant information sharing;

h. new research activities; or

i. activities likely to create serious risks.

15.11 DPIA Contents

A DPIA shall include:

a. description of processing activity;

b. purpose of processing;

c. categories of information involved;

d. individuals affected;

e. assessment of risks;

f. existing safeguards;

g. proposed mitigation measures;

h. approval decisions; and

i. review requirements.

15.12 DPIA Responsibilities

The relevant department shall:

a. identify need for assessment;

b. provide information;

c. implement safeguards; and

d. cooperate with review.

The Data Protection Officer shall:

a. advise on methodology;

b. review assessments;

c. provide recommendations; and

d. maintain DPIA records.

PART V

DATA PROTECTION RISK REGISTER

15.13 Establishment of Risk Register

ILA shall maintain a Data Protection Risk Register to record identified privacy risks.

15.14 Contents of Risk Register

The register shall include:

a. risk description;

b. affected information;

c. affected persons;

d. risk category;

e. likelihood rating;

f. impact rating;

g. overall risk level;

h. existing controls;

i. additional measures required;

j. responsible person;

k. review date; and

l. status.

15.15 Risk Monitoring

Risk owners shall regularly review assigned risks and update:

a. risk status;

b. mitigation actions;

c. emerging threats;

d. control effectiveness; and

e. completion timelines.

PART VI

COMPLIANCE MONITORING FRAMEWORK

15.16 Purpose of Compliance Monitoring

ILA shall monitor compliance to ensure that:

a. policies are implemented;

b. procedures are followed;

c. risks are controlled;

d. staff comply with obligations;

e. weaknesses are identified; and

f. improvements are achieved.

15.17 Compliance Monitoring Activities

Monitoring may include:

a. internal reviews;

b. audits;

c. access reviews;

d. security assessments;

e. documentation checks;

f. training monitoring;

g. incident analysis;

h. stakeholder feedback; and

i. compliance reporting.

PART VII

INTERNAL DATA PROTECTION AUDITS

15.18 Purpose of Internal Audits

ILA shall conduct periodic internal data protection audits to evaluate whether:

a. this Policy is effectively implemented;

b. procedures are being followed;

c. safeguards are functioning;

d. risks are adequately managed;

e. staff comply with responsibilities; and

f. improvements are required.

15.19 Scope of Data Protection Audits

Audits may examine:

a. personal data processing activities;

b. legal case files;

c. beneficiary records;

d. safeguarding information;

c. employee records;

d. financial records;

e. ICT systems;

f. access controls;

g. information-sharing practices;

h. retention and disposal practices;

i. third-party arrangements; and

j. training compliance.

15.20 Audit Frequency

Audits shall be conducted:

a. periodically according to risk level;

b. after significant incidents;

c. when major systems change;

d. when new programmes create significant risks; or

e. where management considers necessary.

15.21 Audit Independence

Where possible, audits shall be conducted by persons who are sufficiently independent from the activity being reviewed.

External expertise may be engaged where:

a. specialized knowledge is required;

b. independence is necessary;

c. risks are significant; or

d. donor requirements apply.

PART VIII

DATA PROTECTION COMPLIANCE ASSESSMENTS

15.22 Compliance Assessments

In addition to formal audits, ILA may conduct compliance assessments to evaluate specific areas of data protection performance.

15.23 Areas of Assessment

Assessments may include:

a. departmental compliance;

b. confidentiality practices;

c. staff awareness;

d. system security;

e. partner compliance;

f. data-sharing arrangements;

g. retention practices;

h. consent procedures; and

i. data subject rights management.

15.24 Assessment Reports

Assessment reports shall identify:

a. findings;

b. risks;

c. weaknesses;

d. good practices;

e. recommendations;

f. responsible persons; and

g. implementation timelines.

PART IX

CORRECTIVE ACTION MANAGEMENT

15.25 Corrective Action Plans

Where weaknesses are identified, ILA shall develop corrective action plans.

15.26 Contents of Corrective Action Plans

Corrective action plans shall specify:

a. identified issue;

b. risk involved;

c. required action;

d. responsible officer;

e. resources required;

f. completion deadline;

g. monitoring arrangements; and

h. status updates.

15.27 Monitoring Corrective Actions

Responsible officers shall provide updates on implementation.

The Data Protection Officer shall monitor progress and escalate unresolved issues.

15.28 Escalation of Outstanding Risks

Unresolved high-risk issues shall be escalated to:

a. Department Head;

b. Executive Director;

c. Data Protection Committee; or

d. Board of Directors where appropriate.

PART X

DATA PROTECTION PERFORMANCE INDICATORS

15.29 Purpose of Indicators

ILA shall use performance indicators to measure effectiveness of its data protection framework.

15.30 Suggested Data Protection Indicators

Indicators may include:

Training Indicators

- percentage of staff completing training;
- number of awareness sessions conducted;
- staff competency assessment results.

Incident Indicators

- number of incidents reported;
- response time;
- number of resolved incidents;
- recurring incidents.

Compliance Indicators

- number of audits completed;
- number of corrective actions completed;
- percentage of departments reviewed.

Rights Management Indicators

- number of data subject requests received;
- response time;
- complaints received;
- requests resolved.

Security Indicators

- access reviews completed;
- system vulnerabilities addressed;
- security assessments conducted.

PART XI

MANAGEMENT REPORTING

15.31 Data Protection Reports

The Data Protection Officer shall prepare periodic reports for management.

15.32 Contents of Reports

Reports may include:

a. compliance status;

b. risk profile;

c. audit findings;

d. incidents;

c. training performance;

d. data subject requests;

e. corrective actions;

f. emerging risks;

g. resource requirements; and

h. recommendations.

15.33 Reporting to the Board

Significant matters shall be presented to the Board, including:

a. serious breaches;

b. major risks;

c. repeated compliance failures;

d. significant legal concerns;

e. resource requirements; and

f. strategic improvements.

PART XII

DATA PROTECTION PERFORMANCE REVIEW

15.34 Annual Review

ILA shall conduct an annual review of its data protection framework.

15.35 Review Areas

The review shall consider:

a. effectiveness of policies;

b. compliance performance;

c. incidents and lessons learned;

d. technological developments;

e. organizational changes;

f. stakeholder feedback;

g. audit outcomes;

h. resource adequacy; and

i. improvement opportunities.

15.36 Outcomes of Review

The review may result in:

a. policy amendments;

b. new procedures;

c. additional training;

d. improved controls;

e. revised risk assessments;

f. organizational changes; or

g. additional resources.

PART XIII

CONTINUOUS IMPROVEMENT FRAMEWORK

15.37 Commitment to Improvement

ILA shall continuously improve its data protection practices through:

a. monitoring;

b. evaluation;

c. audits;

d. incident learning;

e. stakeholder feedback;

f. technological improvements;

g. staff development; and

h. review of international good practices.

15.38 Lessons Learned

Lessons from:

a. incidents;

b. complaints;

c. audits;

d. assessments;

e. programme implementation;

f. partner experiences; and

g. operational challenges

shall be incorporated into future improvements.

PART XIV

COMPLIANCE MONITORING TOOLS AND TEMPLATES

15.39 Compliance Tools

ILA shall maintain practical tools including:

Annex I:

Data Protection Risk Assessment Template

Annex II:

Data Protection Risk Register Template

Annex III:

Data Protection Impact Assessment Template

Annex IV:

Data Protection Audit Checklist

Annex V:

Corrective Action Tracking Form

Annex VI:

Data Protection Compliance Review Report Template

Annex VII:

Annual Data Protection Performance Report Template

CHAPTER SIXTEEN

DATA PROTECTION POLICY IMPLEMENTATION, REVIEW AND AMENDMENT

16.1 Introduction

The Initiative for Legal Aid (ILA) recognizes that the effectiveness of this Data Protection and Privacy Policy depends not only on its approval but also on consistent implementation, monitoring, review, and continuous improvement.

This Chapter establishes the framework for:

a. implementing the Policy;

b. assigning ownership and accountability;

c. communicating requirements;

d. reviewing effectiveness;

e. managing amendments;

f. controlling versions; and

g. ensuring continued relevance and compliance.

PART I

POLICY IMPLEMENTATION FRAMEWORK

16.2 Implementation Commitment

ILA shall implement this Policy through:

a. organizational leadership;

b. assigned responsibilities;

c. operational procedures;

d. staff training;

e. technical safeguards;

f. monitoring mechanisms;

g. compliance reviews; and

h. continuous improvement initiatives.

16.3 Implementation Responsibility

Overall responsibility for implementation rests with the Executive Director, supported by:

a. Data Protection Officer;

b. Data Protection Committee;

c. Legal Department;

d. ICT Department;

e. Human Resources Department;

f. Programme Departments;

g. MEAL Unit;

h. Safeguarding Unit; and

i. all personnel.

16.4 Operationalization of the Policy

ILA shall operationalize this Policy through:

a. standard operating procedures;

b. staff guidance notes;

c. confidentiality agreements;

d. data processing procedures;

e. security protocols;

f. retention schedules;

g. incident reporting mechanisms;

h. training programmes; and

i. monitoring tools.

PART II

POLICY OWNERSHIP

16.5 Policy Owner

The owner of this Policy shall be the Executive Director of ILA.

The Executive Director shall ensure that:

a. the Policy remains effective;

b. adequate resources are available;

c. responsibilities are assigned;

d. compliance is monitored; and

e. improvements are implemented.

16.6 Technical Ownership

The Data Protection Officer shall serve as the technical custodian of this Policy.

The DPO shall:

a. maintain the Policy;

b. provide interpretation guidance;

c. coordinate implementation;

d. monitor compliance;

e. recommend revisions;

f. maintain records; and

g. support awareness activities.

PART III

POLICY APPROVAL AND EFFECTIVE DATE

16.7 Approval Authority

This Policy shall be approved by the Board of Directors of ILA or another authorized governance body.

16.8 Effective Date

This Policy shall take effect on the date approved by the authorized approving authority.

16.9 Binding Nature

Upon approval, this Policy shall be binding on:

a. employees;

b. volunteers;

c. interns;

d. consultants;

e. contractors;

f. partners where applicable; and

g. any person processing information on behalf of ILA.

PART IV

POLICY COMMUNICATION AND ACCESSIBILITY

16.10 Communication of Policy

ILA shall ensure that this Policy is communicated to relevant stakeholders.

Communication may occur through:

a. staff induction;

b. training sessions;

c. internal communications;

d. organizational platforms;

e. partner briefings; and

f. awareness activities.

16.11 Accessibility of Policy

ILA shall ensure that the Policy is accessible to persons who require knowledge of its provisions.

Where appropriate, simplified guidance materials may be developed.

PART V

POLICY REVIEW

16.12 Periodic Review Requirement

This Policy shall be reviewed periodically to ensure that it remains:

a. relevant;

b. effective;

c. compliant with applicable requirements;

d. aligned with organizational operations;

e. responsive to risks; and

f. consistent with good practice.

16.13 Review Frequency

The Policy shall ordinarily be reviewed:

a. at least once every two years; or

b. earlier where circumstances require.

16.14 Circumstances Requiring Earlier Review

An earlier review may occur where there is:

a. significant legal change;

b. major organizational restructuring;

c. serious data breach;

d. introduction of new technology;

e. significant programme expansion;

f. audit findings;

g. donor requirements; or

h. identified weaknesses.

PART VI

POLICY AMENDMENT PROCEDURES

16.15 Authority to Amend

Amendments to this Policy shall be approved by the appropriate authority in accordance with ILA governance procedures.

16.16 Amendment Process

Proposed amendments shall consider:

a. operational experience;

b. legal developments;

c. audit findings;

d. incident lessons;

e. stakeholder feedback;

f. technological changes; and

g. organizational needs.

16.17 Documentation of Amendments

All amendments shall be documented, including:

a. date of amendment;

b. description of changes;

c. reason for amendment;

d. approving authority;

e. effective date; and

f. responsible person.

PART VII

VERSION CONTROL

16.18 Policy Version Management

ILA shall maintain version control to ensure that only approved versions of this Policy are in use.

16.19 Version Control Information

The Policy shall include:

Version	Date Approved	Description of Changes	Approved By
Version 1.0	[Insert Date]	Initial Approval	Board of Directors

16.20 Withdrawal of Previous Versions

Superseded versions shall be:

a. removed from active circulation;

b. archived appropriately;

c. retained for institutional records; and

d. clearly marked as outdated.

PART VIII

POLICY EXCEPTIONS

16.21 Requests for Exceptions

Exceptional circumstances may require temporary deviation from this Policy.

Any exception request shall:

a. identify the requirement affected;

b. explain the justification;

c. assess risks;

d. identify mitigation measures;

e. specify duration; and

f. obtain approval.

16.22 Approval of Exceptions

Exceptions involving significant privacy risks shall require approval from:

a. Data Protection Officer;

b. Legal Department;

c. Executive Director; or

d. Board of Directors where necessary.

16.23 Recording Exceptions

All approved exceptions shall be documented in an Exception Register containing:

a. nature of exception;

b. justification;

c. approval authority;

d. risk assessment;

e. mitigation measures; and

f. expiry date.

PART IX

INTERPRETATION AND GUIDANCE

16.24 Interpretation Authority

Questions concerning interpretation of this Policy shall be referred to the Data Protection Officer in consultation with the Legal Department.

16.25 Conflict with Other Policies

Where this Policy conflicts with another ILA policy relating to information management, confidentiality, safeguarding, ICT, or records management, the matter shall be reviewed to determine the appropriate approach.

16.26 Alignment with Other Policies

This Policy shall be implemented together with relevant ILA policies, including:

a. Safeguarding and PSEA Policy;

b. Code of Conduct and Ethics Policy;

c. ICT Policy;

d. Financial and Accounting Policy;

e. Human Resource Manual;

f. MEAL Policy;

g. Procurement Policy;

h. Risk Management Policy; and

i. Anti-Fraud, Corruption and Whistleblowing Policy.

PART X

FINAL PROVISIONS

16.27 Commitment to Privacy Protection

ILA commits to protecting personal data as an essential component of:

a. human dignity;

b. access to justice;

c. ethical service delivery;

d. organizational integrity;

e. safeguarding; and

f. responsible governance.

16.28 Compliance Obligation

Failure to comply with this Policy may result in:

a. corrective action;

b. withdrawal of access privileges;

c. disciplinary action;

d. contractual consequences;

e. reporting obligations; or

f. other appropriate measures.

16.29 Entry into Force

This Policy shall remain in force until amended, replaced, or withdrawn by the competent authority of ILA.