REPUBLIC OF KENYA

# COUNCIL OF LEGAL EDUCATION

# DATA PROTECTION POLICY

## 2024

# COPYRIGHT

**All rights reserved**

Copyright © 2024

by **The Council of Legal Education**

## TABLE OF CONTENTS

## TABLE OF CONTENTS

## FOREWORD

The Council of Legal Education (CLE) is a State Corporation established by the Legal Education Act, Cap. 16B of Laws of Kenya. CLE has been in existence since 2014 when it formally separated from the Kenya School of Law. It is mandated to regulate, supervise and license legal education programmes and legal education providers in Kenya. In addition, it administers the Advocates Training Programme (ATP) examination for purposes of admission to the Roll of Advocates in Kenya and advises the Government on matters germane to legal education and training.

In light of the above, CLE works with stakeholders to deliver this mandate by ensuring efficient service delivery. In the process, CLE collects personal information from stakeholders who including both individuals and organizations. These stakeholders include: candidates sitting for the Bar examination, applicants who apply for the equation for foreign qualifications and legal education providers, job seekers', visitors, the Council, staff, and service providers' personal information.

In today's rapidly evolving digital landscape, the protection of personal data is paramount. As we continue to embrace technological advancements and data-driven decision-making, CLE must handle the stakeholders' personal information with the utmost care and integrity. CLE's commitment to safeguarding privacy is not only a legal obligation but also a reflection of our dedication to building trust and ensuring transparency in all our operations.

This Data Protection Policy outlines the measures we have adopted to ensure the confidentiality, integrity, and availability of personal data under our care. It establishes the principles that guide our data collection, processing, storage, and sharing practices, ensuring compliance with applicable data protection laws and regulations, specifically the Data Protection Act, 2019 and its Regulations. Additionally, it underscores our commitment to protecting individual rights and maintaining the highest standards of data security.

By adhering to this Policy, we not only mitigate risks associated with data breaches but also foster a culture of responsibility and respect for privacy across the organization.

## FOREWORD

Our goal is to create a secure environment where personal data is handled with the care it deserves, empowering our stakeholders with the confidence that their information is protected.

We encourage our stakeholders to familiarize themselves with this Policy and adhere to its provisions. Together, we can ensure that data protection remains a cornerstone of our operations, promoting ethical data management and enhancing our reputation as a trustworthy and responsible entity.

**Prof. Collins Odote Oloo**
**CHAIRPERSON**
**COUNCIL OF LEGAL EDUCATION**

## ACKNOWLEDGMENT

This Data Protection Policy has been developed to provide clear guidance on how personal data is processed within CLE. It sets out the principles that underpin our approach to data privacy and security, and it defines the roles and responsibilities of every member of our team in safeguarding the information entrusted to us.

The Policy is a living document and will be reviewed as data protection standards evolve and new technologies emerge. All CLE stakeholders will be expected to read understand and adhere to the Policy to ensure that we protect and uphold the data privacy of the concerned subjects.

I wish to thank the Data Protection Committee, which spearheaded the development of this Policy. Also, I extend sincere gratitude to our staff members and other external stakeholders who contributed to its successful formulation by giving invaluable feedback to immensely better the Policy.

Additionally, I acknowledge the Management for providing essential resources and leadership throughout the initiative, as well as the Council for engaging in meaningful discussions and ultimately ratifying the Policy.

The development of this Policy was further enriched by the invaluable insights and support from the Office of the Data Protection Commissioner (ODPC), whose collaboration and guidance ensured that the Policy aligned with the relevant legal and regulatory frameworks.

I am confident that the provisions outlined in this Policy will significantly aid in the effective implementation of data protection measures at CLE.

**Ms. Jennifer Gitiri, HSC**
**AG. SECRETARY/CEO**
**COUNCIL OF LEGAL EDUCATION**

## APPROVAL

This Council deliberated dully adopted and approved this Data Protection Policy in its meeting held on the 14th day of October 2024.

The Council will review this Policy from time to time. All amendments will be communicated in writing using the Amendment Sheet. This will ensure that the Policy will remain consistent with the CLE mandate.

**Chairperson**
**COUNCIL OF LEGAL EDUCATION**

**Ag. Secretary/Chief Executive Officer**
**COUNCIL OF LEGAL EDUCATION**

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## POLICY AMENDMENT SHEET

| Issue/Revision No | Subject of Amendments | Reviewed By (Signature) | Review Authorized By (Signature) | Date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |


## ABBREVIATIONS AND ACRONYMS

**AGPO** Access to Government Procurement Opportunities

**AI** Artificial Intelligence

**ERP** Enterprise Resource Planner

**CLE** Council of Legal Education

**DPIA** Data Protection Impact Assessment

**DPO** Data Protection Officer

**GDPR** General Data Protection Regulation

**HELB** Higher Education Loans Board

**ICT** Information and Communication Technology

**IoT** Internet of Things

## DEFINITION OF TERMS

**Act:** means the Data Protection Act, 2019 that makes provision for the regulation of the processing of personal data;

**Anonymisation:** means the removal of personal identifiers from personal data so that the data subject is no longer identifiable;

**Biometric Data:** means personal data resulting from specific technical processing based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

**Confer:** means to discuss something important in order to make a decision;

**Contracted professional:** means a person engaged by CLE to offer services to the mandate, mostly for on short-term basis e.g. peer reviewers, setters, markers, moderators, invigilators, quality assurers;

**Council:** means the Board of Council of Legal Education;

**Consent:** means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject;

**Data:** means information which:

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system;

(d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or

(e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

**Data Commissioner:** means the person appointed to oversee the implementation of the Data Protection Act;

**Data Controller:** means a natural or legal person, public authority, agency or otherbody which, alone or jointly with others, determines the purpose and means of processing of personal data;

**Data Processor**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

## DEFINITION OF TERMS

**Data Protection:** means the fair and proper use of information about data subjects;

**Data Protection Committee**: means the organizational structure of CLE that advocates and implements data protection issues and is appointed by the CEO/Secretary. It is comprised of a chairperson, secretary and members;

**Data Protection Officer**: means an officer with the relevant academic qualifications and skills, appointed by the CEO/Secretary to ensure that CLE processes data subject's personal data in accordance with the applicable data protection rules;

**Data Protection Impact Assessment (DPIA):** means an assessment of the impact of the envisaged processing operations on the protection of personal data. This is done where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes;

**Data Subject**: means an identified or identifiable natural person who is the subject of personal data. They include current and potential candidates, job seekers, the Council, CLE staff, service providers and visitors;

**Encryption:** means the process of converting the content of any readable data using technical means into coded form;

**Health data:** means data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services;

**Identifiable Natural Person**: means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

**Person**: means an individual who has attained the age of eighteen years;

**Personal data**: means any information relating to an identified or identifiable natural person e.g. health information, address, name, income, cultural profile etc.;

**Personal Data Breach**: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

**Privacy**: means the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively;

## DEFINITION OF TERMS

**Processing:** means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as:

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

**Pseudonymisation:** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

**Register:** means the register kept and maintained by the Data Commissioner under section 21 of the Act;

**Restriction of Processing:** means the marking of stored personal data with the aim of limiting their processing in the future;

**Sensitive Personal Data:** means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject;

**Staff:** means an employee of Council of Legal Education;

**Supplier:** means a person that provides a product or service to Council of Legal Education;

**Third Party:** means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data;

**Visitor:** refers to a person visiting Council of Legal Education offices;

**Website:** refers to the Council of Legal Education website, www.cle.or.ke;

## CLE VISION, MISSION, CORE VALUES AND STRATEGIC GOAL

### Vision

Innovative Legal Professionals Transforming Society

### Mission

To ensure quality legal education through responsive regulation and administration of Bar Examination

### Core Values

The Council of Legal Education will uphold the following values;

- Accountability
- Excellence
- Integrity
- Inclusiveness
- Innovation

### Strategic Goal

- Transformative legal education and training in Kenya


# INTRODUCTION

## 1.1. Background

The Constitution of Kenya provides for the Right to Privacy, a fundamental human right that must be upheld. Specifically, Article 31(c) and (d) of the Constitution, gives effect to the Data Protection Act, 2019 and its 2021 Regulations, which set out how data processers and controllers should process personal data while upholding the rights of data subjects. These legal and regulatory frameworks also provide for penalties to data processors and controllers when personal data breaches occur.

CLE as an entity, collects personal data through different media, that is, manually and through the use of information, communication and technological platforms, hence it is expected to abide with the legal and regulatory frameworks that pertains to data protection. Further, the rapid advancement of technologies like, systems, artificial intelligence (AI), big data analytics, and the Internet of Things (IoT), increases the amount of data collected and the complexity of managing it. Additionally, in today's interconnected world, personal data often crosses borders.

With the foregoing, it is crucial for personal data to be protected at all costs, due to the growing need of this asset for gainful use by both entities and individuals. In addition, the increasing awareness among individuals about the value and sensitivity of their personal data has driven a demand for better privacy protection. People are increasingly concerned about how their information is used, shared, or sold, especially without their consent.

This Data Protection Policy therefore responds to the apparent risks that CLE can be exposed to while handling personal data and it places a strong emphasis on individual privacy rights. The implementation of this Policy, not only responds to legal compliance but it also strives to maintain stakeholders' trust. This Policy addresses the fair and proper use of personal and sensitive personal data for CLE stakeholders and it demonstrates how CLE will collect, use, share, store and protect personal data.

## 1.2. Policy Rationale

In the past, CLE has not had a comprehensive workplace policy on data protection. This necessitated the development of this workplace policy that will provide a systematic guideline on the implementation of the CLE data protection mainstreaming workplace response. Further, the development of this Policy was necessitated by the enactment of the Data Protection Act in 2019 and the Data Protection (General) Regulations in 2021.

## 1.3. Policy Statement

CLE is committed to ensuring the privacy and protection of all personal data that it handles in compliance with the Constitution of Kenya, the Data Protection Act, and the Data Protection (General) Regulations.

This policy statement sets the foundation for Data Protection, highlighting the organization's dedication to protecting personal data, complying with laws, and fostering trust with stakeholders.

CLE commits to implementing this Policy by allocating the necessary resources in order to achieve and maintain data protection within and without the organization.

## 1.4. Policy Goal, Objectives and Scope

### 1.4.1. Policy Goal

To ensure the lawful, transparent, and secure handling of personal data within CLE, in compliance with the applicable laws and regulations.

### 1.4.2. Policy Objectives

The objective of this Policy is to:

i. stipulate the handling or processing of personal data;

ii. ensure that the processing of personal data of a data subject is guided by the principles set out the Data Protection Act;

iii. protect the privacy of individuals/stakeholders;

iv. establish the legal and institutional mechanism to protect personal data; and

v. provide data subjects/stakeholders with rights and remedies to protect their personal data from processing that is not in accordance with the applicable laws and regulations.

### 1.4.3. Policy Scope

This Policy applies to the Council, CLE staff and stakeholders.

## 1.5 Legal and Regulatory Framework

This policy is informed by the provisions of the:

i. Constitution of Kenya

ii. Computer Misuse and Cybercrimes Act

iii. Data Protection Act

iv. Data Protection (General) Regulations

v. General Data Protection Regulation (GDPR-EU)

## 1.6. Guiding Principles

CLE shall ensure that personal data is:

i. processed in accordance with the right to privacy of the data subject;

ii. processed lawfully, fairly and in a transparent manner in relation to any data subject;

iii. collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

iv. adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

v. collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

vi. accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

vii. kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

viii. not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

## 2. POLICY PROVISIONS

### 2.1. Data Protection System/Data Protection by Design and by Default

2.1.1. CLE shall implement appropriate technical and organizational measures (as outlined in below) which are designed:

a. to implement the data protection principles effectively; and

b. to integrate necessary safeguards for that purpose into the processing.

2.1.2. Technical and organizational measures to be implemented include:

3.1.2.1. CLE shall register with the Data Commissioner as well as maintain the registration according to the provisions of the Act. Where there are changes in particulars, CLE shall notify the Data Commissioner of the change(s);

2.1.2.2. The CEO/Secretary shall appoint a data protection committee to guide, manage, monitor and evaluate the process of data protection integration into mainstreaming culture, policies and programmes in CLE. The composition of the Committee shall include a Chairperson, Secretary and members who shall be drawn from different and relevant functions of CLE;

2.1.2.3. The CEO/Secretary shall appoint a data protection officer with relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection;

2.1.2.4. CLE shall publish the contact details of the data protection officer on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website;

2.1.2.5. CLE shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration:

a. the amount of personal data collected;

b. the extent of its processing;

c. the period of its storage;

d. its accessibility; and

e. the cost of processing data and the technologies and tools used.

2.1.2.6. CLE shall identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;

2.1.2.7. CLE shall establish and maintain appropriate safeguards against the identified risks;

2.1.2.8. CLE shall pseudonymise and encrypt personal data;

2.1.2.9. CLE shall restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

2.1.2.10. CLE shall verify that they are effectively implemented; and

2.1.2.11. CLE shall ensure that the safeguards are continually updated in response to new risks or deficiencies.

## 2.2. Rights of Data Subjects

A data subject has a right to:

a. be informed of the use to which their personal data is to be put;

b. access their personal data in the custody of data controller or data processor;

c. object to the processing of all or part of their personal data;

d. correction of false or misleading data; and

e. deletion of false or misleading data about them.

## 2.3. Conferred Rights of Data Subjects

A right conferred on a data subject may be exercised:

## 2.4. Obligations of Data Subjects

Data subjects shall:

a. Not unreasonably or unjustifiably withhold consent for use of personal data collected by the CLE;

b. Give consent authorizing CLE to their personal data, take images, videography therefrom and use such personal data for an individual or group sense without the need for redaction of any particular data subject or personal data related to the group ;

c. If the data subject separates from the CLE, CLE shall continue using the photos, videos and other personal data of the data subject in so far as is necessary or on receipt of an erasure or objection.

## 2.5. Collection of Personal Data

2.5.1. CLE shall:

a. Obtain consent from data subjects before processing of personal data;

b. Ensure that the data subject is informed in a language they understand while obtaining consent;

c. Ensure that the consent is voluntarily given and is specific;

d. Ensure that the data subject has the capacity to understand and communicate their consent;

2.5.2. CLE shall, before collecting personal data, in so far as practicable, inform the data subject of:

a. the rights of data subject specified under paragraph 3.2 and 3.3. above;

b. the fact that personal data is being collected;

c. the purpose for which the personal data is being collected;

d. the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;

e. the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

f. a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;

g. the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and

h. the consequences if any, where the data subject fails to provide all or any part of the requested data.

2.5.3. CLE shall collect personal data directly from the data subject;

2.5.4. Despite (2.5.3) above, personal data may be collected indirectly where:

a. the data is contained in a public record;

b. the data subject has deliberately made the data public;

c. the data subject has consented to the collection from another source;

d. the data subject has an incapacity, the guardian appointed has consented to the collection from another source;

e. the collection from another source would not prejudice the interests of the data subject;

f. collection of data from another source is necessary:

(i) for the prevention, detection, investigation, prosecution and punishment of crime;

(ii) for the enforcement of a law which imposes a pecuniary penalty; or

(iii) for the protection of the interests of the data subject or another person.

2.5.5. CLE shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.

## 2.6. Conditions of Consent

2.6.1. CLE shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose;

2.6.2. Unless otherwise provided under this Policy, a data subject shall have the right to withdraw consent at any time;

2.6.3. The withdrawal of consent in 3.6.2. above, shall not affect the lawfulness of processing based on prior consent before its withdrawal;

2.6.4. In determining whether consent was freely given, account shall be taken on whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

## 2.7. Data Collection Channels, Reasons for Collection and Safeguards

2.7.1. CLE collects personal data and sensitive personal data from the Council, CLE staff, potential and current candidates, job seekers, visitors and service providers through the following channels:

a. Electronic platforms e.g. the Enterprise Resource Planner (portals), website etc;

b. Completed manual application forms and attendance forms provided by CLE;

c. Visitors signing in the visitors' book;

d. CCTV cameras located within CLE premises;

e. Photography, filming and other data capture methods during CLE activities;

f. Recording information of data subjects who make calls to CLE;

2.7.2. CLE collects personal data and sensitive personal data for the following reasons:

a. To fulfil the statutory and regulatory requirements of regulating, supervising and licensing legal education programmes and providers in Kenya, setting standards for curriculum and modular instruction, setting standards for modes and quality of examinations, setting standards for harmonization of legal education programmes in Kenya and the region, monitoring and evaluating legal education providers and programmes, administering the Bar examination and advising the Government on matters relating to legal education;

b. To facilitate disbursement of the Bar Education Loan through the partner institution, HELB;

c. To enable communication with stakeholders hence improving service delivery, customer service and creating customer value;

d. To support staff in the performance of their duties;

e. Recruitment purposes.

2.7.3. To ensure confidentiality, integrity, and availability of personal data and sensitive personal data, CLE has implemented the following technical and organizational measures:

a. Access controls and authentication mechanisms to prevent unauthorized access to personal data;

b. Installation of firewalls and intrusion prevention and detection systems to prevent unauthorized access to ICT systems;

c. Encryption of personal data to protect against unauthorized disclosure;

d. Regular backups and disaster recovery procedures including a Business Continuity Plan to ensure the availability of personal data;

e. Monitoring and logging of access to personal data to detect and respond to security incidents;

## 2.8. Lawful Processing of Personal Data

2.8.1. CLE shall not process personal data, unless:

a. the data subject consents to the processing for one or more specified purposes; or

b. the processing is necessary:

i. for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;

ii. for compliance with any legal obligation to which the data controller is subject;

iii. to protect the vital interests of the data subject or another natural person;

iv. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

v. for the exercise, by any person in the public interest, of any other functions of a public nature;

vi. for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

vii. for historical, statistical, journalistic, literature and art or scientific research;

2.8.2. Further processing of personal data shall be per the purpose of collection.

## 2.9. Processing of personal data relating to a Minor

2.9.1 CLE shall not process personal data relating to a minor unless:

a. consent is given by the child's parent or guardian; and

b. the processing is in such a manner that protects and advances the rights and best interests of the child.

2.9.2 CLE shall incorporate appropriate mechanisms for age verification and consent to process personal data of a child;

2.9.3 Mechanisms contemplated under paragraph 3.9.2. shall be determined based on:

a. available technology;

b. the volume of personal data processed;

c. the proportion of such personal data likely to be that of a child;

d. possibility of harm to a child arising out of the processing of personal data; and

e. such other factors as may be specified by the Data Commissioner.

## 2.10. Restrictions of Processing Personal Data

2.10.1 CLE shall, at the request of a data subject, restrict the processing of personal data where:

a. accuracy of the personal data is contested by the data subject, for a period enabling CLE to verify the accuracy of the data;

b. personal data is no longer required for the processing unless CLE requires the personal data for the establishment, exercise or defence of a legal claim;

c. processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

d. data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor override those of the data subject.

2.10.2 Where processing of personal data is restricted under this section:

a. the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

b. CLE shall inform the data subject before withdrawing the restriction on the processing of personal data.

2.10.3 CLE shall respond to requests of rectification, erasure or restriction of processing of personal data within seven (7) days after receipt of the request.

## 2.11. Data Breach Management and Notification

2.11.1 CLE shall receive any suspected or actual data breaches from the public;

2.11.2 Where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the data subject whose personal data has been subjected to the unauthorised access, CLE shall;

a. notify the Data Commissioner without delay, within seventy-two (72) hours of becoming aware of such breach;

b. communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established.

However, communication of a breach to the data subject shall not be required, where CLE has implemented appropriate security safeguards which may include encryption of affected personal data;

c. carry out a breach detection and analysis;

d. carry out containment, eradication and recovery;

e. carry out a post incident investigation and develop a report on the breach.

2.11.3 Where the notification to the Data Commissioner is not made within seventy-two (72) hours, the notification shall be accompanied by reasons for the delay;

2.11.4 CLE may delay or restrict communication referred to under paragraph 3.11.3. above, as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body;

2.11.5 The notification and communication referred to under paragraph 3.11.2 (b) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including:

a. description of the nature of the data breach;

b. description of the measures that CLE intends to take or has taken to address the data breach;

c. recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

d. where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data; and

e. the name and contact details of the data protection officer where applicable or another contact point from whom more information could be obtained.

2.11.6 CLE shall record the following information about a personal data breach:

a. the facts relating to the breach;

b. its effects; and

c. the remedial action taken.

## 2.12 Commercial use of data

2.12.1. CLE shall not use, for commercial purposes, personal data obtained from a data subject pursuant to the provisions of this Policy unless the person;

a. has sought and obtained the express consent from a data subject; or

b. is authorised to do so under any written law, and the data subject has been informed of such use when collecting the data from the data subject.

2.12.2. Where CLE uses personal data for commercial purposes, it shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.

## 2.13 Data Sharing

2.13.1. CLE shall receive and share personal data with other government agencies to enable fulfilment of its mandate;

2.13.2. CLE may receive a data sharing code issued by the Data Commissioner containing practical guidance on the sharing of personal data according to provisions of the Data Protection Act. The data sharing code will specify on the lawful exchange of personal data between government departments or public sector agencies.

## 2.14 Transfer of Personal Data Outside Kenya and Safeguards

2.14.1 CLE may transfer personal data to another country only where:

a. CLE has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data and the appropriate safeguards including jurisdictions with commensurate data protection laws;

b. the transfer is necessary:

i. for the performance of a contract between the data subject and CLE or implementation of precontractual measures taken at the data subject's request;

ii. for the conclusion or performance of a contract concluded in the interest of the data subject between CLE and another person;

iii. for any matter of public interest;

iv. for the establishment, exercise or defence of a legal claim;

v. in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

vi. for the purpose of compelling legitimate interests pursued by CLE which are not overridden by the interests, rights and freedoms of the data subjects.

2.14.2 CLE shall process sensitive personal data out of Kenya only upon obtaining consent from the data subject and on obtaining confirmation of appropriate safeguards.

## 2.15 Data Protection Impact Assessment (DPIA)

2.15.1. CLE shall, prior to a project that will interact with personal data, carry out a DPIA;

2.15.2. CLE shall also conduct Data Protection Impact Assessment on a case-to-case basis where the processing of personal data is likely to result in a high risk to the rights and freedoms of data subjects;

2.15.3. The DPIA shall include the following:

a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor;

b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c. an assessment of the risks to the rights and freedoms of data subjects;

d. the measures envisaged to address the risks and the safeguards, security

measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act and its Regulations, taking into account the rights, and legitimate interests of data subjects and other persons concerned.

2.15.4. CLE shall consult the Data Commissioner prior to the processing if a data protection impact assessment prepared under this section indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject;

2.15.5. The data impact assessment reports shall be submitted sixty days before the processing of data;

2.15.6. CLE shall be guided by the Data Commissioner guidelines for carrying out an impact assessment under this section.

## 2.16 Disclosure of Personal Data Collected

2.16.1 CLE shall seek consent from data subjects before disclosure to third parties;

2.16.2 CLE shall disclose personal data pursuant to legal requirements;

2.16.3 CLE shall not monetize personal data to third parties;

2.16.4 The interested party shall make an official request for the disclosure of personal data to the CEO/Secretary, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure;

## 2.17 Processing of Sensitive Personal Data

2.17.1 CLE shall process the sensitive personal data of an individual only where:

a. the processing is carried out in the course of legitimate activities with appropriate safeguards on condition that:

   i. the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and

   ii. the personal data is not disclosed outside that body without the consent of the data subject.

b. the processing relates to personal data which is manifestly made public by the data subject; or

c. processing is necessary for:
   i. exercise or defence of a legal claim;
   ii. the purpose of carrying out the obligations and exercising specific rights of CLE or of the data subject; or
   iii. protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

2.17.2 Personal data relating to the health of a data subject may only be processed:
   a. by or under the responsibility of a health care provider; or
   b. by a person subject to the obligation of professional secrecy under any law.

2.17.3 Where external institutions are used to process personal data on behalf of CLE, the

responsibility for the security and appropriate use of that data shall remain with CLE;

2.17.4 Where a third-party data processor is used:
   a. a data processor shall be appointed to provide sufficient security measures to protect the data;
   b. reasonable steps shall be taken to ensure security measures are in place; and
   c. a written and signed contract establishing what personal data shall be processed and for what purpose shall be set out.

2.17.5 The external Institutions shall be made aware of the Data Protection Policy and shall guarantee CLE that they understand and acknowledge that any disclosure and/or appropriation of any confidential information as well as the violation of the legal requirements regarding the protection of the processing of personal data, are of a nature to the cause of serious and irreparable damage to CLE. Such violation shall attract penalties stipulated in the contract and the Kenyan Laws on data protection.

## 2.18 Retention and Disposal of Personal Data

2.18.1 CLE shall retain personal data as guided by the CLE Retention and Disposal Policy;

2.18.2 CLE shall retain and use personal data to the extent necessary to comply with legal obligations.

## 2.19. Capacity Building

2.19.1. CLE shall sensitize staff, train management and the Data Protection Committee on data protection and how to mainstream the same in CLE;

2.19.2. CLE shall leverage opportunities presented by knowledge management processes including identifying, creating, storing, sharing, using, learning and improving to enhance the workplace data protection mainstreaming response;

2.19.3. CLE shall undertake benchmarking with an aim of identifying opportunities for improvement on data protection mainstreaming initiatives/interventions at CLE.

## 2.20. Partnerships and Collaborations

CLE shall engage in partnerships and collaborations to improve and promote data protection interventions and programs in CLE.

## 2.21. Resources

2.21.1. CLE shall ensure adequate financial and human resources allocation to data protection interventions annually;

2.21.2. CLE shall provide the necessary equipment and technology to support data protection interventions to enhance the data protection mainstreaming outcomes;

## 2.22. Policy Non-Compliance

2.22.1. Non-compliance occurs when there is a failure to adhere to the provisions and obligations of this Policy. This may include:

a. Unauthorized processing or disclosure of personal data;
b. Breach of confidentiality agreements;
c. Failure to implement required technical measures;
d. Ignoring or by-passing consent requirements for data collection and processing; and
e. Non-compliance with the data retention and disposal protocols.

2.22.2. Non-compliance incidents must be reported to the Data Protection Officer (DPO) immediately. The DPO will document the incident and initiate a review process

to assess the severity of the breach. All incidents will be escalated to the Data Protection Committee, which will oversee the investigation and recommend corrective measures;

2.22.3. The Data Protection Committee will ensure that all corrective actions are implemented and reported to the CEO/Secretary;

2.22.4. Stakeholders who do not comply with this Policy will be sanctioned as guided by the relevant laws and regulations and the CLE Human Resources Policy, whichever is applicable.

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## 3. POLICY IMPLEMENTATION

Implementation of this policy will require the collaboration of various players. The roles and responsibilities of specific organs and individuals include;

### 3.1. The Council

The Council shall:

i. Approve the Data Protection Policy;

ii. Approve resources for implementation of this Policy;

iii. Provide feedback to management in regards to data protection;

### 3.2. CLE Staff

CLE Employees shall:

i. Report any form data breach to any member of the mainstreaming committee or the Accounting Officer;

ii. Meaningfully contribute and participate in data protection programs.

### 3.3. Stakeholders

CLE stakeholders shall endeavor to uphold the guiding principles and provisions outlined in this Policy.

### 3.4. Data Protection Committee

The Data Protection Committee shall:

i. Implement all data protection interventions;

ii. Strengthen data protection capacities among CLE employees;

iii. Develop the annual report for data protection interventions at CLE;

iv. Submit periodic reports to the relevant oversight body(ies);

v. Ensure CLE is in good standing with the Data Commissioner;

vi. Monitor and evaluate data protection activities in CLE;

vii. Conduct data protection committee meetings at least once every six (6) months;

viii. Review this data protection policy and strategies;

ix. Carry out advocacy and lobbying to enhance data protection achievements at CLE;

x. Mobilize resources to support data protection initiatives at CLE;

xi. Establish and strengthen networks with partners on data protection and privacy issues;

xii. Plan and budget for data protection programmes while ensuring the efficient use of resources allocated for data protection activities;

xiii. Advice the Management on data protection issues;

xiv. Effectively communicate data protection issues and interventions;

xv. Ensure that this Policy aligns with other policies;

xvi. Sensitize staff and management on data protection issues.

### 3.5. Data Protection Officer

The Data Protection Officer shall:

i. Advise CLE on data processing requirements provided under the Act or any other written law;

ii. ensure on behalf of the data controller or data processor that the Act is complied with;

iii. facilitate capacity building of staff involved in data processing operations;

iv. provide advice on data protection impact assessment; and

v. co-operate with the Data Commissioner and any other authority on matters relating to data protection.

## 4. POLICY MONITORING, REPORTING AND REVIEW

### 4.1. Compliance

This Policy shall be communicated to all staff and relevant stakeholders. All staff with management responsibility shall ensure compliance with the provisions of this policy within their directorates and divisions.

### 4.2. Monitoring and Evaluation

Implementation monitoring of this Policy shall be undertaken by the Data Protection Committee to ensure its effectiveness, efficiency, sustainability, and relevance. Periodic evaluation will be undertaken to assess the impact of this policy by the relevant division according to the Monitoring and evaluation framework of CLE.

### 4.3. Policy Reporting

The Committee shall provide annual reports on the progress of the implementation of this Data Protection Policy to the CEO/Secretary.

### 4.4. Policy Review

4.4.1. This policy shall be reviewed as necessary;

4.4.2. Any amendment or modification to this Policy will remain effective from the date of ratification of the amendment.

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## Appendix I: Candidate Consent Form

REPUBLIC OF KENYA

**COUNCIL OF LEGAL EDUCATION**

**CONSENT FORM FOR CANDIDATE PERSONAL DATA**

The Council of Legal Education (CLE) is committed to protecting candidates' personal data registering for the ATP examination. In compliance with the Data Protection Act, 2019, CLE requires your consent to collect, process, store, and share your personal data for registration of the Bar examination and for gazettement purposes.

This consent form explains how your personal data will be handled throughout the process and provides you with an overview of your rights regarding your data.

**1.Purpose of Data Collection**

The personal data you provide will be collected and processed solely for the purpose of sitting for the ATP examination. This includes evaluating your academic qualifications.

**2. Personal Data and sensitive personal to be collected**

- Full Name
- Student numbers
- Identification Documents (e.g., National ID or Passport)
- Date of birth
- Nationality
- County
- Marital status
- Gender
- Legal Education Provider Firm and Class
- Contact Information (Address, Email Address, Mobile Number)
- University attended
- Next of kin details

- Passport photo
- Disability status
- Copy of the O-Level certificate
- Copy of the A-Level certificate
- Copy of CLE clearance letter
- Copy of KNQA clearance
- Copy of the national identification card or passport bio-data page
- Copy of the university degree certificate (LL.B)
- Copy of the university transcripts
- Legal Education provider admission letter

**3. Use of Personal Data**

Your personal data will be used for the following purposes:

- Fulfilling legal obligations related to the ATP programme
- Contacting you regarding your application status

**4. Data Sharing**

Your personal data may be shared with other government agencies as required by law for compliance purposes. In such cases, these third parties shall be obligated to protect your data in accordance with the Data Protection Act, 2019.

**5. Data Security and Retention**

CLE is committed to ensuring the security and confidentiality of your personal data. Your data will be stored securely in compliance with ICT standards and protocols as well as CLE's Records and Archives Management Policy.

**6. Data Subject Rights**

Candidates have the following rights:

- The right to access and request a copy of the data held by CLE
- The right to request correction of any inaccuracies in your data
- The right to withdraw consent for data processing at any time, although this may affect your application status
- The right to request the deletion of data

**7. Complaints**

If you believe that CLE has violated your data protection rights or failed to comply with the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

**8. Contact Information**

For any inquiries regarding this consent form or to withdraw consent, please contact:

Data Protection Officer

Council of Legal Education

dpo@cle.or.ke

**Applicant Declaration**

By signing this form, I confirm that I have read, understood, and agree to the collection, processing, and storage of my personal data by the Council of Legal Education. Tick accordingly.

**___ gives consent** **___ does not give consent**

**Name of Candidate**.....

**Candidate Number:** .....

**Signature:** .....

**Date:** .....

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## Appendix Ii: Recognition and Approval of Foreign Legal Qualifications Consent Form

REPUBLIC OF KENYA

**COUNCIL OF LEGAL EDUCATION**

**CONSENT FORM FOR PROCESSING REGONTION AND APPROVAL OF FOREIGN LEGAL QUALIFICATION PERSONAL DATA**

The Council of Legal Education (CLE) is committed to protecting personal data applying for recognition and approval of foreign legal qualifications. In compliance with the Data Protection Act, 2019, CLE requires your consent to collect, process, store, and share your personal data for registration purposes.

This consent form explains how your personal data will be handled throughout the process and provides you with an overview of your rights regarding your data.

**1.Purpose of Data Collection**

The personal data you provide will be collected and processed solely for the above-mentioned process.

**2. Personal Data and sensitive personal to be Collected**

- Full Name
- Date Of Birth
- Postal Address
- Mobile Number
- Nationality
- Email Address
- Academic Qualifications
- Copies of Original and Certified Copies Of Academic Certificates

**3. Use of Personal Data**

Your personal data will be used for the following purposes:

- Fulfilling legal obligations related to the ATP programme
- Contacting you regarding your application status

**4. Data Sharing**

Your personal data may be shared with other government agencies as required by law for compliance purposes. In such cases, these third parties shall be obligated to protect your data in accordance with the Data Protection Act, 2019.

**5. Data Security and Retention**

CLE is committed to ensuring the security and confidentiality of your personal data. Your data will be stored securely in compliance with ICT standards and protocols as well as CLE's Records and Archives Management Policy.

**6. Data Subject Rights**

Applicants have the following rights:

- The right to access and request a copy of the data held by CLE
- The right to request correction of any inaccuracies in your data
- The right to withdraw consent for data processing at any time, although this may affect your application status
- The right to request the deletion of data

**7. Complaints**

If you believe that CLE has violated your data protection rights or failed to comply with the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

**8. Contact Information**

For any inquiries regarding this consent form or to withdraw consent, please contact:

Data Protection Officer

Council of Legal Education

dpo@cle.or.ke

**Applicant Declaration**

By signing this form, I confirm that I have read, understood, and agree to the collection, processing, and storage of my personal data by the Council of Legal Education. Tick accordingly.

**___ gives consent** **___ does not give consent**

**Name** .....

**Signature:** .....

**Date:** .....

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## Appendix Iii: Suppliers Consent Form


**COUNCIL OF LEGAL EDUCATION**

**SUPPLIERS CONSENT FORM FOR PROCESSING PERSONAL DATA**

The Council of Legal Education (CLE) is committed to protecting suppliers' personal data. In compliance with the Data Protection Act, 2019, CLE requires your consent to collect, process, store, and share your personal data for registration purposes.

This consent form explains how your personal data will be handled throughout the procurement process and provides you with an overview of your rights regarding your data.

**1. Purpose of Data Collection**

The personal data you provide will be collected and processed solely for the above-mentioned process.

**2. Personal Data and sensitive personal to be Collected**

- Full Name
- Postal Address
- Mobile Number
- Email Address
- Name(s) of directors
- Location
- Copy of the PIN Certificate
- Copy of the Certificate of Registration
- Copy of the Certificate of Incorporation
- Copy of the Tax Compliance Certificate
- Copy of the Trade Licence
- Copy of the AGPO Certificate

**3. Use of Personal Data**

Your personal data will be used for the following purposes:

- Procurement process evaluation
- Contacting you

**4. Data Sharing**

Your personal data may be shared with other government agencies as required by law for compliance purposes. In such cases, these third parties shall be obligated to protect your data in accordance with the Data Protection Act, 2019.

**5. Data Security and Retention**

CLE is committed to ensuring the security and confidentiality of your personal data. Your data will be stored securely in compliance with ICT standards and protocols as well as CLE's Records and Archives Management Policy.

**6. Data Subject Rights**

Suppliers have the following rights:

- The right to access and request a copy of the data held by CLE
- The right to request correction of any inaccuracies in your data
- The right to withdraw consent for data processing at any time, although this may affect your application status
- The right to request the deletion of data

**7. Complaints**

If you believe that CLE has violated your data protection rights or failed to comply with the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

**8. Contact Information**

For any inquiries regarding this consent form or to withdraw consent, please contact:

Data Protection Officer

Council of Legal Education

dpo@cle.or.ke

**Applicant Declaration**

By signing this form, I confirm that I have read, understood, and agree to the

collection, processing, and storage of my personal data by the Council of Legal Education. Tick accordingly.

**___ gives consent** **___ does not give consent**

**Name** .....

**Company:** .....

**Signature:** .....

**Date:** .....

**Supply of:** .....

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise



**COUNCIL OF LEGAL EDUCATION**

**CONTRACTED PROFESSIONALS CONSENT FORM FOR PROCESSING PERSONAL DATA**

The Council of Legal Education (CLE) is committed to protecting contracted professionals' personal data. In compliance with the Data Protection Act, 2019, CLE requires your consent to collect, process, store, and share your personal data for registration purposes.

This consent form explains how your personal data will be handled throughout the service provision process as a contracted professional and provides you with an overview of your rights regarding your data.

**1. Purpose of Data Collection**

The personal data you provide will be collected and processed solely for the above-mentioned process.

**2. Personal Data and sensitive personal to be Collected**

- Full Name
- Postal Address
- Mobile Number
- Email Address
- Academic Qualifications and copies
- Occupation
- Work history
- PIN Certificate
- Vehicle log book (where necessary)

**3. Use of Personal Data**

Your personal data will be used for the following purposes:

- Service provision
- Contacting you

**4. Data Sharing**

Your personal data may be shared with other government agencies as required by law for compliance purposes. In such cases, these third parties shall be obligated to protect your data in accordance with the Data Protection Act, 2019.

**5. Data Security and Retention**

CLE is committed to ensuring the security and confidentiality of your personal data. Your data will be stored securely in compliance with ICT standards and protocols as well as CLE's Records and Archives Management Policy.

**6. Rights of Applicants**

Contracted professionals have the following rights:

- The right to access and request a copy of the data held by CLE
- The right to request correction of any inaccuracies in your data
- The right to withdraw consent for data processing at any time, although this may affect your application status
- The right to request the deletion of your data

**7. Complaints**

If you believe that CLE has violated your data protection rights or failed to comply with the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

**8. Contact Information**

For any inquiries regarding this consent form or to withdraw consent, please contact:

Data Protection Officer

Council of Legal Education

dpo@cle.or.ke

**Applicant Declaration**

By signing this form, I confirm that I have read, understood, and agree to the

collection, processing, and storage of my personal data by the Council of Legal Education. Tick accordingly.

**___ gives consent** **___ does not give consent**

**Name:** .....

**Signature:** .....

**Date:** .....

**Activity:** .....

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## Appendix V: Stakeholder Consent Form


**COUNCIL OF LEGAL EDUCATION**

**STAKEHOLDER CONSENT FORM FOR PROCESSING PERSONAL DATA**

The Council of Legal Education (CLE) is committed to protecting its stakeholders' personal data. In compliance with the Data Protection Act, 2019, CLE requires your consent to collect, process, store, and share your personal data for registration purposes.

This consent form explains how your personal data will be handled and provides you with an overview of your rights regarding your data.

**1.Purpose of Data Collection**

The personal data you provide will be collected and processed solely for this event and publicity on CLE media platforms.

**2. Personal Data and sensitive personal to be Collected**

- Full Name
- Mobile Number
- Email Address
- Organization
- Photograph
- Videography

**3. Use of Personal Data**

Your personal data will be used for the following purposes:

- Internal and external reporting
- Publicity

**4. Data Sharing**

Your personal data may be shared with other government agencies as required by law for compliance purposes. In such cases, these third parties shall be obligated to protect your data in accordance with the Data Protection Act, 2019.

**5. Data Security and Retention**

CLE is committed to ensuring the security and confidentiality of your personal data. Your data will be stored securely in compliance with ICT standards and protocols as well as CLE's Records and Archives Management Policy.

**6. Rights of Applicants**

Stakeholders have the following rights:

- The right to access and request a copy of the data held by CLE
- The right to request correction of any inaccuracies in your data
- The right to withdraw consent for data processing at any time, although this may affect your application status
- The right to request the deletion of your data

**7. Complaints**

If you believe that CLE has violated your data protection rights or failed to comply with the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

**8. Contact Information**

For any inquiries regarding this consent form or to withdraw consent, please contact:

Data Protection Officer

Council of Legal Education

dpo@cle.or.ke

**Applicant Declaration**

By signing this form, I confirm that I have read, understood, and agree to the collection, processing, and storage of my personal data by the Council of Legal

Education. My consent is given freely without expecting payment and I therefore agree not to seek any payment from CLE.

**Name:** .....

**Signature:** .....

**Date:** .....

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

## Appendix Vi: Staff Consent Form


**COUNCIL OF LEGAL EDUCATION**

**STAFF CONSENT FORM**

The Council of Legal Education (CLE) is committed to safeguarding your personal data in compliance with the Data Protection Act, 2019. In accordance with the legal mandate, CLE requires your consent to collect, store, process, and share your personal data. This consent form outlines the nature and purpose of the data we collect and how it will be used.

**1. Purpose of Data Collection**

Your personal data will be collected to enable you to provide services to CLE and to ensure compliance with the legal and regulatory requirements governing CLE's operations.

**2. Personal Data to Be Collected**

The categories of personal data that may be collected and used by CLE include:

- Full Name
- Physical Address
- Email Address
- Mobile Number
- Personal Identification Numbers
- Academic Qualifications
- Work History
- Certification Documents
- Any other information necessary for employment purposes

**4. Use of Personal Data**

Your personal data will be used strictly for the following purposes:

- Employment and contractual obligations
- Ensuring compliance with legal requirements
- Processing payroll, benefits, and taxes
- Record keeping in accordance with CLE policies
- Communication of official CLE matters

**5. Data Sharing**

Your personal data may be shared with other government agencies as mandated by law for compliance and legal obligations, as well as with third parties such as insurance providers to facilitate the provision of coverage in accordance with CLE policies.

**6. Data Storage and Security**

CLE will store your personal data securely in accordance with ICT standards, protocols, and record retention requirements. All necessary safeguards will be implemented to protect your data from unauthorized access, loss, or misuse.

**7. Rights to Access, Correct, and Withdraw Consent**

- right to access your personal data at any time.
- right to request the correction of any inaccurate or incomplete data.
- right to withdraw consent to the processing of your data at any time, but this may affect CLE's ability to fulfil its legal or contractual obligations.
- right to request the deletion of data

**8.Complaints**

If you believe that CLE has violated this consent or the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

By signing this consent form, you acknowledge that you have read, understood, and agreed to the terms outlined herein.

**Employee Declaration**

I, _____, hereby give my consent for the Council of Legal Education to collect, process, store, and share my personal data as described in this form. I understand that I may withdraw my consent at any time by contacting CLE, but I also understand that this may impact my ability to provide services to CLE.

Signature: _____

Date: _____

Employee ID: _____

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

REPUBLIC OF KENYA

## COUNCIL OF LEGAL EDUCATION

## CONSENT FORM FOR PROCESSING RECRUITMENT DATA

The Council of Legal Education (CLE) is committed to protecting the personal data of individuals applying for positions within the organization. In compliance with the Data Protection Act, 2019, CLE requires your consent to collect, process, store, and share your data for recruitment purposes.

This consent form explains how your personal data will be handled throughout the recruitment process and provides you with an overview of your rights regarding your data.

### 1.Purpose of Data Collection

The personal data you provide will be collected and processed solely for the purpose of recruitment. This includes evaluating your qualifications, experience, and suitability for the position you have applied for, as well as contacting you during the recruitment process.

### 2. Personal Data to Be Collected

The following categories of personal data may be collected during the recruitment process:

- Full Name
- Contact Information (Address, Email Address, Mobile Number)
- Personal Identification Numbers
- Ethnicity
- Academic Qualifications and Transcripts
- Professional Certifications
- Work History and References

- Curriculum Vitae (CV)
- Identification Documents (e.g., National ID or Passport)
- Any other relevant information necessary to assess your application

**3. Use of Personal Data**

Your personal data will be used for the following purposes:

- Assessing your suitability for the position applied for
- Verifying the information provided in your application
- Contacting you regarding your application status
- Conducting background checks, where necessary
- Fulfilling legal and regulatory obligations related to employment

**4. Data Sharing**

Your personal data may be shared with other government agencies as required by law for compliance purposes. Additionally, third parties such as background verification service providers or recruitment agencies may be engaged to assist with the recruitment process. In such cases, these third parties will be obligated to protect your data in accordance with the Data Protection Act, 2019.

**5. Data Security and Retention**

CLE is committed to ensuring the security and confidentiality of your personal data. Your data will be stored securely in compliance with ICT standards and protocols. If your application is successful, your data will be transferred to your employment records. If your application is not successful, your data will be retained for a limited period for potential future opportunities unless you request its deletion.

**6. Rights of Applicants**

You have the following rights with respect to your personal data:

- The right to access and request a copy of the data held by CLE
- The right to request correction of any inaccuracies in your data
- The right to withdraw consent for data processing at any time, although this may affect your application status
- The right to request the deletion of your data if you are not selected for the position

**7. Complaints**

If you believe that CLE has violated your data protection rights or failed to comply with the Data Protection Act, 2019, you may file a complaint with CLE's Data Protection Officer or the Office of the Data Protection Commissioner.

**8. Contact Information**

For any inquiries regarding this consent form or to withdraw consent, please contact:

Data Protection Officer

Council of Legal Education

dpo@cle.or.ke

**Applicant Declaration**

By signing this form, I confirm that I have read, understood, and agree to the collection, processing, and storage of my personal data by the Council of Legal Education for recruitment purposes. I understand that I may withdraw my consent at any time, but I acknowledge that this may affect my application for employment.

Applicant Name: _____

Signature: _____

Date: _____

Position Applied For: _____

HARAMBEE
REPUBLIC OF KENYA
Council of Legal Education
Setting Standards for Legal Education
Regulate • License • Supervise

REPUBLIC OF KENYA

# COUNCIL OF LEGAL EDUCATION


**The Council of Legal Education,**
P.O Box 829 - 00502,
Karen Office Park Karen,
Nairobi, Kenya.

**020-6980100**

**info@cle.or.ke**

**0719150000**

**www.cle.or.ke**