ASSOCIATION OF COMPUTING PRACTITIONERS-KENYA(ACPK)

P.O.Box 28209 - 00100 Nairobi | Coop House | Info@acpk.or.ke | www.acpk.or.ke
0724064794 | 0720 343 201 | 0722 942 376

ACPK WEBSITE AND MEMBER PORTAL PRIVACY NOTICE

Document Reference: ACPK-DP-PN-001
Version: 1.0
Data Controller: Association of Computing Practitioners Kenya (ACPK)
Website: https://acpk.or.ke
Privacy Contact: kacpinfo@gmail.com
Effective Date: 04/11/2026

1. Introduction

The Association of Computing Practitioners Kenya (ACPK) is committed to protecting personal data and respecting the privacy rights of all individuals who interact with its website, membership portal, professional development services, events and digital platforms.

This Privacy Notice explains how ACPK collects, uses, stores, shares, protects and retains personal information, and how individuals may exercise their data protection rights.

ACPK processes personal data in accordance with the Kenya Data Protection Act, 2019, the applicable Data Protection Regulations, 2021, and the GDPR where applicable.

2. Scope

This Notice applies to:

a) ACPK members and membership applicants.
b) Website and member portal users.
c) Conference, workshop and event participants.
d) Training, CPD and professional recognition applicants.
e) Sponsors, partners and service provider representatives.
f) Individuals who communicate or transact with ACPK.

3. Personal Data We Collect

Depending on the service requested, ACPK may collect:

a) Identity and contact information: Full name, email address, telephone number, postal address and other necessary identification details.

b) Professional information: Employer, job title, professional qualifications, certifications, professional experience, membership history and professional recognition records.

c) Membership information: Membership number, category, subscription status, registration history and membership-related transactions.

d) Financial and transaction information: Subscription payments, event fees, invoices, transaction references and payment confirmation records. ACPK shall not require members to disclose mobile money PINs, card PINs or other payment authentication secrets.

e) Professional development information: Training enrolment, attendance, CPD records, assessment results, certificates and digital credentials.

f) Technical information: IP addresses, authentication records, device and browser information, security logs and cookies or similar technologies where used.

g) Communication preferences: Subscription preferences, event notifications and optional marketing consent records.

ACPK shall avoid collecting sensitive personal data unless necessary, lawful and supported by appropriate safeguards.

4. Purposes and Lawful Basis of Processing

ACPK processes personal data for the following purposes, subject to the applicable lawful basis:

Processing purpose	Applicable lawful basis
Membership registration and administration	Membership agreement/contract or other established lawful basis
Subscription processing and financial records	Contractual necessity and legal obligations
Professional qualification verification	Contractual necessity, legitimate interests or consent, as appropriate
Training, CPD and event administration	Contractual necessity or consent, as applicable

Professional recognition and digital badges	Contractual necessity or another documented lawful basis; separate consent where required
Essential membership communications	Contractual necessity, legal obligation or legitimate interests, as applicable
Optional promotional communications	Valid consent where required
Website security and fraud prevention	Legitimate interests or legal obligations, as applicable
Regulatory reporting and statutory records	Legal obligations
Anonymous or aggregated service analytics	Where genuinely anonymized, outside personal data processing; otherwise an appropriate lawful basis is required

ACPK shall determine and document the appropriate lawful basis before undertaking each processing activity.

Consent shall not be treated as the universal legal basis for all membership administration.

5. Data Sharing and Disclosure

ACPK may disclose necessary personal information to authorized recipients, including:

a) Contracted website hosting and IT service providers.
b) Authorized payment processing service providers.
c) Training and certification partners where necessary.
d) Event service providers where necessary.
e) Regulatory or law enforcement authorities where legally required.
f) Other recipients specifically authorized by the individual or otherwise permitted by law.

ACPK shall not sell member personal information or disclose member contact lists to sponsors for independent commercial marketing without a valid lawful basis and the required permissions.

Access to member information shall be limited according to approved roles and legitimate operational needs.

6. International Data Transfers

Where personal data is stored, accessed or processed outside Kenya, ACPK shall ensure that applicable cross-border data transfer requirements are satisfied.

This may include appropriate contractual safeguards, lawful transfer mechanisms, applicable regulatory requirements and additional technical protections.

Where GDPR applies, transfers subject to Chapter V shall use an appropriate adequacy decision, safeguard or lawful derogation.

7. Data Retention

ACPK shall retain personal data only for the period necessary to fulfil the purposes for which it was collected, subject to applicable legal, financial, contractual and legitimate recordkeeping requirements.

Retention periods shall be established in an approved Data Retention Schedule.

At the end of the applicable retention period, personal data shall be securely deleted, anonymized or archived where legally justified.

8. Data Security

ACPK shall implement appropriate technical and organizational measures, including:

a) Role-based access controls.
b) Secure authentication and password protection.
c) Encryption where appropriate.
d) Secure transmission of information.
e) Access monitoring and audit logging.
f) Security updates and vulnerability management.
g) Data backup and recovery measures.
h) Incident response and breach management.
i) Confidentiality obligations for authorized personnel.

Although ACPK shall take reasonable measures to protect information, no internet-based service can guarantee absolute security.

9. Individual Data Protection Rights

Subject to applicable law, individuals may exercise the following rights:

a) To be informed about the collection and use of their personal data.
b) To request access to personal information held about them.
c) To request correction of inaccurate or misleading information.
d) To object to certain processing activities.
e) To request deletion where legally applicable.
f) To withdraw consent where processing is based on consent.
g) To request restriction of processing or data portability where applicable under the GDPR.
h) To challenge certain solely automated decisions where applicable.

Requests may be submitted through ACPK's designated privacy contact.

ACPK may request reasonable verification of identity before processing a request.

10. Consent and Communication Preferences

Where consent is required, ACPK shall obtain a freely given, specific, informed and unambiguous indication of the individual's wishes.

Consent shall be recorded and may be withdrawn through an accessible mechanism.

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

Members may opt out of optional promotional communications without losing access to essential membership services.

11. Cookies and Website Analytics

ACPK may use strictly necessary cookies to support website operation, authentication and security.

Where optional analytics, advertising or tracking technologies are used, ACPK shall provide appropriate information and obtain consent where required by applicable law.

Users shall be able to manage applicable cookie preferences.

12. Personal Data Breaches

ACPK shall investigate suspected personal data breaches and implement appropriate containment, assessment and remediation measures.

Where legally required, ACPK shall notify the Office of the Data Protection Commissioner and affected individuals within the applicable statutory requirements.

Where GDPR applies, ACPK shall additionally comply with relevant supervisory authority and data subject notification obligations.

13. Children and Vulnerable Individuals

ACPK shall apply appropriate safeguards when processing information relating to children or other vulnerable individuals.

Where parental or guardian authorization is legally required, ACPK shall obtain and verify the necessary authorization.

14. Third-Party Websites

ACPK's website may contain links to external websites or services.

ACPK does not control the privacy practices of independent third-party websites. Users are encouraged to review their respective privacy notices.

15. Complaints and Enquiries

Individuals who have concerns about the processing of their personal data may contact:

ACPK Data Protection Contact
Email: elvinamugu@gmail.com | kacpinfo@gmail.comm

16. Changes to This Notice

ACPK may update this Privacy Notice to reflect legal, regulatory, technological or operational changes.

P.O.Box 28209 - 00100 Nairobi | Coop House | Info@acpk.or.ke | www.acpk.or.ke
0724064794 | 0720 343 201 | 0722 942 376

Material changes shall be communicated through appropriate channels.

The latest approved version shall be published on the ACPK website.