



MYDREAMCV.COM

DATA PROTECTION AND PRIVACY POLICY

1. Introduction

MyDreamCV.com is committed to protecting the privacy, confidentiality and security of personal information entrusted to us by our clients, website visitors, prospective customers, job seekers, business partners and other individuals.

We recognise that CV writing, resume development and career-branding services require individuals to share personal and professional information that may be confidential. Such information may include employment history, academic qualifications, contact details, professional achievements, career objectives, references and other details necessary to prepare accurate and effective career documents.

This Data Protection and Privacy Policy establishes the principles, procedures and safeguards governing the collection, use, storage, disclosure, retention and disposal of personal data by MyDreamCV.com.

We process personal data in accordance with applicable data protection laws, including the Constitution of Kenya, the Data Protection Act, 2019, and the applicable regulations made under that Act. Where we process information belonging to individuals in other jurisdictions, we will comply with additional data protection requirements where applicable.

By using our website, requesting our services or voluntarily providing personal information to us, you acknowledge that you have been given an opportunity to read this Policy. Where consent is the appropriate legal basis for processing, we will obtain that consent separately where necessary.

2. Scope of the Policy

This Policy applies to personal data processed in connection with accessing or browsing mydreamcv.com; requesting quotations or making enquiries; purchasing or receiving CV and resume writing services; requesting cover letters, LinkedIn profile optimisation, executive profiles, career-change CVs or related career-branding services; receiving interview coaching or career consultations; communicating by email, telephone, WhatsApp, website forms or other approved channels; making payments, requesting invoices or receiving support; applying for employment or contractual opportunities with MyDreamCV; and subscribing to newsletters or consenting to marketing communications.

This Policy applies to personal data processed electronically, in physical documents and through other business communication channels.

3. Data Controller and Contact Details

For purposes of this Policy, the entity that determines why and how personal data is processed is the data controller. MyDreamCV.com is operated by Savvy Concepts. The relevant legal entity responsible for processing personal data shall be identified as follows:

Business name: Savvy Concepts
Trading name: MyDreamCV.com
Website: <https://mydreamcv.com>
Privacy enquiries: dataprivacy@mydreamcv.com
General enquiries: cv@mydreamcv.com
Telephone/WhatsApp: +254 720 079413

Where another organisation processes personal data on our behalf, it will act as a data processor subject to appropriate contractual and legal safeguards.

4. Personal Data We Collect

4.1 Identification and contact information: Full name and preferred name; telephone number and email address; country, city and other relevant location information; postal address where required; professional website or LinkedIn profile URL; and other contact information voluntarily supplied by the client.

4.2 Career and professional information: Existing CVs and resumes; employment history, job titles and responsibilities; educational qualifications, certifications and professional licences; skills, competencies and career achievements; professional references and referee contact details; career objectives, target positions and preferred industries; employment gaps and career-transition information; publications, projects, awards and professional memberships; and information contained in job advertisements or application instructions provided by clients.

4.3 Supporting documents: Clients may voluntarily provide certificates, academic transcripts, professional licences, recommendation letters, identification documents or other supporting records. We will request or use these documents only where reasonably necessary. Clients should avoid submitting national identity numbers, passport details, financial account information or other sensitive information unless specifically necessary and requested through an appropriate secure channel.

4.4 Payment and transaction information: Payment confirmations, transaction references, invoices, service descriptions, payment status and billing information. Payments may be handled by third-party providers. We will not intentionally collect or retain complete payment-card security credentials unless a lawful and necessary arrangement specifically permits it.

4.5 Website and technical information: Depending on website configuration and consent choices where required, we may collect IP address, browser and device type, operating system, pages visited, referral source, approximate session duration, website error logs, security events, diagnostic information, cookie identifiers and website preferences.

4.6 Communications and feedback: Enquiries, correspondence, service instructions, client feedback, complaints, revision requests and records of decisions necessary to manage service delivery and resolve disputes.

4.7 Sensitive personal data: Some information may qualify as sensitive personal data under applicable law, including information revealing health status, ethnic or social origin, religious or philosophical beliefs, biometric information, family circumstances or other legally protected categories. We do not routinely require sensitive personal data to prepare a CV. Where such information is genuinely necessary, we will apply additional safeguards and obtain the appropriate lawful basis or consent where required.

5. How We Collect Personal Data

We collect personal data directly from clients through CVs, questionnaires, documents, forms and instructions; through email, telephone, WhatsApp and other communication channels; through website enquiry and service forms; through payment providers or financial institutions that supply transaction confirmations; from authorised third parties where clients permit us to receive information; and through website technologies where enabled and lawful.

We do not knowingly obtain personal data through unlawful means or encourage clients to submit another person's information without appropriate authority.

6. Purposes for Processing Personal Data

6.1 Service delivery: To prepare, edit, review and improve CVs, resumes, cover letters, executive profiles, LinkedIn profiles and related career documents according to clients' instructions.

6.2 Customer relationship management: To respond to enquiries, provide quotations, communicate project requirements, clarify information, manage revisions and deliver completed documents.

6.3 Payments and administration: To confirm payments, issue invoices, maintain transaction records, manage refunds where applicable and fulfil legitimate accounting and tax obligations.

6.4 Quality assurance: To check document accuracy, manage quality-control processes, maintain service records and address complaints or requests for corrections.

6.5 Website security and performance: To prevent fraud, detect unauthorised access, maintain system integrity, troubleshoot technical problems and improve website functionality.

6.6 Marketing and business development: Where lawful, we may send information about our services, career resources, promotions or relevant updates. We will respect applicable consent requirements and provide a practical means of opting out of direct marketing.

6.7 Legal compliance and dispute resolution: To comply with applicable laws, respond to lawful requests, establish or defend legal claims and protect our legitimate business interests.

We will not use personal data for a new purpose that is incompatible with the original purpose unless an appropriate legal basis or other lawful authorisation permits it.

7. Lawful Basis for Processing

We will identify and rely on an appropriate legal basis for each processing activity, as required by applicable law. Depending on the circumstances, this may include performance of a contract; compliance with a legal obligation; consent where it is the appropriate basis; legitimate interests where those interests do not override individuals' rights and freedoms; or another lawful ground recognised by applicable law.

Where we rely on consent, individuals may withdraw it at any time. Withdrawal does not invalidate processing lawfully carried out before withdrawal, and it does not prevent processing that may continue under another valid legal basis.

We will not treat a person's decision to decline optional marketing as a reason to deny an otherwise available service.

8. Confidentiality of CVs and Career Documents

MyDreamCV recognises that CVs and career documents often contain confidential personal and professional information. Client documents will be used primarily to deliver the service requested; access will be restricted to authorised personnel and service providers who need the information; and we will not sell client CVs, resumes, certificates, contact details or other personal data.

We will not disclose client documents to prospective employers, recruiters, referees or other third parties without the client's instructions or another valid legal basis. We will not publish identifiable client CVs, testimonials or career histories as marketing material without appropriate permission or another valid legal basis.

We will not use identifiable client documents to train public artificial intelligence models or create unrelated commercial products without the necessary lawful authority. We will take reasonable measures to ensure downloaded, emailed or otherwise delivered documents are sent to the intended recipient.

Clients should ensure information supplied to us is accurate and that they are authorised to share any third-party information contained in their documents. Confidentiality does not prevent disclosures required by law or disclosures reasonably necessary to establish, exercise or defend legal claims, subject to applicable safeguards.

9. Artificial Intelligence and Automated Tools

Where MyDreamCV uses artificial intelligence, automated writing tools, grammar checkers or other digital services to support document preparation, we will take reasonable steps to protect personal data.

Where applicable, we will use tools only for authorised and relevant service purposes; assess the privacy and security arrangements of external providers; limit personal data submitted to what is necessary; avoid submitting unnecessary sensitive information; apply appropriate contractual, technical and organisational safeguards; and provide additional information or obtain consent where required by law or the nature of the processing.

We will not knowingly permit an external provider to use identifiable client documents for unrelated purposes or model training contrary to applicable contractual commitments or legal requirements.

CV recommendations and document preparation remain subject to appropriate human review. We do not guarantee employment, interview invitations or selection outcomes.

10. Disclosure and Sharing of Personal Data

We may share personal data only where necessary and lawful with authorised staff and contractors involved in service delivery; technology providers such as website hosting, cloud storage, email, document-processing and cybersecurity providers; payment providers; professional advisers; public authorities and regulators where disclosure is required or authorised by law; and other recipients authorised by the client.

We will seek appropriate confidentiality commitments, data-processing terms and security safeguards from third-party providers where required.

We do not sell or rent personal data to data brokers, advertisers, recruiters or employers. Any disclosure for advertising or other commercial purposes will be subject to applicable law and the commitments stated in this Policy.

11. International Data Transfers

MyDreamCV may use service providers or digital platforms that store or process personal data outside Kenya. International transfers may also arise when serving clients in other countries.

Where personal data is transferred outside Kenya, we will comply with applicable Kenyan legal requirements, including requirements relating to appropriate safeguards, lawful transfer conditions and any required consent or authorisation.

Safeguards may include contractual protections, assessment of the recipient's data protection arrangements, appropriate technical measures and other legally recognised transfer mechanisms. Where another jurisdiction's data protection laws apply, we will assess and implement additional transfer protections required by those laws.

Clients may contact us for further information about relevant international transfers, subject to legitimate confidentiality and security restrictions.

12. Data Security Measures

We will implement reasonable technical and organisational measures designed to protect personal data against unauthorised access, loss, misuse, alteration, destruction or disclosure. Measures may include access controls and restricted user permissions; strong passwords and multi-factor authentication where available; encryption in transit and, where appropriate, at rest; secure website connections and appropriate platform configurations; anti-malware protection, software updates and security monitoring; secure document-sharing methods and controlled file access; confidentiality obligations for staff and contractors; secure backup and recovery arrangements; periodic review of data access and security practices; and secure deletion or destruction when information is no longer required.

Security measures will be proportionate to the sensitivity, volume and risks associated with the personal data processed. No electronic transmission or storage system can be guaranteed to be completely secure. We will nevertheless take reasonable steps to reduce risks and respond appropriately to security incidents.

13. Data Retention and Secure Disposal

We retain personal data only for as long as reasonably necessary to fulfil the purposes for which it was collected, meet legal obligations, resolve disputes and protect legitimate interests. The following are proposed operational retention periods and must be aligned with actual systems and legal obligations before adoption:

Unconverted enquiries and quotations: up to 12 months after the last meaningful contact.

Working CVs and supporting documents: up to 90 days after completion of the service.

Final deliverables and revision records: up to 12 months after completion, unless a different period is agreed or necessary.

Invoices and financial records: for the period required by applicable tax, accounting and other laws.

Marketing subscription records: until withdrawal of consent or the end of the applicable retention period.

Security logs and technical records: for a period proportionate to security needs and applicable law.

Complaints and legal records: for as long as reasonably necessary to resolve the matter and meet legal obligations.

When personal data is no longer required, we will take reasonable steps to delete, anonymise or securely destroy it. Residual copies in backups may remain temporarily until overwritten or securely removed under our backup cycle, unless earlier removal is technically feasible or legally required.

Where a client requests earlier deletion, we will assess the request in accordance with applicable law and explain any lawful reason for retaining particular records.

14. Cookies and Website Tracking

MyDreamCV may use cookies and similar technologies to operate the website, remember preferences, improve performance, measure usage and maintain security. These may include essential cookies necessary for core functions; preference cookies; analytics cookies; and advertising or marketing technologies, but only where implemented and subject to applicable consent and legal requirements.

Where required, we will request consent before placing non-essential cookies or activating non-essential tracking technologies. Visitors may manage their choices through available cookie controls and browser settings. Blocking certain cookies may affect website functionality. Actual cookie practices will be described in a cookie notice or settings interface where appropriate.

15. Direct Marketing and Communications

We may use contact information to respond to enquiries, provide service updates and communicate about an ongoing engagement. We will send promotional communications only where permitted by applicable law and will respect required consent or objection.

Individuals may opt out of marketing communications by using an unsubscribe link, where available, or contacting us directly. We will act on valid requests within the applicable legal timeframe.

Opting out of marketing will not prevent us from sending essential communications about an existing order, payment, security matter or legal obligation.

16. Rights of Data Subjects

Subject to applicable law and any lawful limitations, individuals may exercise the following rights: the right to be informed about collection and use; the right of access; the right to correction of inaccurate, incomplete or misleading information; the right to deletion where legal conditions are satisfied; the right to object to particular processing; the right to restriction where legally available; the right to data portability where applicable; the right to withdraw consent where processing is based on consent; the right to complain to the Office of the Data Protection Commissioner in Kenya or another competent authority; and applicable rights concerning decisions made solely by automated processing that have legal or similarly significant effects.

These rights are subject to conditions, exceptions and procedures established by applicable law. A deletion request, for example, may not require us to destroy records that must lawfully be retained.

17. How to Exercise Your Rights

To exercise a data protection right, submit a request using the privacy contact details in Section 3. Include your name and preferred contact details; a description of the personal data or processing activity concerned; the right you wish to exercise and the action requested; and sufficient information to enable us to locate relevant records.

We may request proportionate information to verify your identity or authority to act on behalf of another person. We will not request unnecessary identity documents.

We will acknowledge, assess and respond to requests within the time limits prescribed by applicable law. If further information is needed, a request cannot be fulfilled in full, or we are legally entitled to refuse it, we will explain the position and available complaint or review options.

You may also contact the Office of the Data Protection Commissioner through its official website: <https://www.odpc.go.ke/>.

18. Personal Data Breaches

A personal data breach may involve unauthorised access, accidental disclosure, loss, destruction, alteration or misuse of personal information. Where a suspected breach occurs, we will investigate and assess the incident; contain it and prevent further unauthorised access; determine the categories and approximate number of individuals affected; assess likely consequences and risks; notify relevant authorities and affected individuals where required by law; take remedial action and document the incident; and review and strengthen controls to reduce recurrence.

We will comply with applicable breach-notification requirements and deadlines, including statutory requirements governing notification to the Data Commissioner and affected individuals where applicable.

Affected individuals should contact our designated privacy contact if they suspect their information has been exposed, lost or misused.

19. Third-Party Websites and Services

Our website or communications may contain links to third-party websites, job boards, recruitment platforms, payment services or professional networks. Those services operate under their own terms and privacy policies. MyDreamCV is not responsible for independent processing carried out by third parties outside our control.

We encourage users to review third-party privacy notices before submitting personal information to those services.

20. Children's Personal Data

Our services are primarily intended for adults seeking career-development assistance. Where we receive personal data relating to a child, including a student or school leaver, we will process it only where lawful and subject to applicable parental or guardian authorisation, age-related requirements and additional safeguards.

We do not knowingly collect children's personal data for unrelated marketing or profiling purposes.

21. Responsibilities of Staff and Contractors

Any staff member or contractor authorised to handle personal data must use it only for approved business purposes; maintain confidentiality during and after their engagement; follow approved access-control and information-security procedures; avoid storing client documents on unauthorised personal devices or accounts; use approved channels for receiving and transmitting client information; report suspected breaches, accidental disclosures or unauthorised access promptly; and comply with applicable data protection laws and relevant internal procedures.

Access to personal data may be suspended or withdrawn where a security or confidentiality risk is identified.

22. Data Protection Governance and Accountability

MyDreamCV will maintain proportionate governance arrangements to support compliance with applicable data protection requirements. These may include maintaining an inventory of personal data processing activities; documenting purposes and legal bases; reviewing data processors and relevant contracts; maintaining a retention and secure-disposal schedule; assessing risks associated with new systems; conducting privacy or data protection impact assessments where required; providing appropriate privacy training; maintaining procedures for data subject requests and complaints; reviewing this Policy and associated controls periodically; and determining and meeting applicable registration obligations with the Office of the Data Protection Commissioner.

Where the law requires the appointment of a Data Protection Officer or another designated privacy role, we will make the necessary arrangements.

23. Complaints and Dispute Resolution

Individuals who believe MyDreamCV has processed their personal data improperly may submit a complaint using the privacy contact details in Section 3. We will review complaints fairly, investigate relevant facts and communicate the outcome within the applicable timeframe.

If an individual is dissatisfied with our response, they may refer the matter to the Office of the Data Protection Commissioner or another competent authority where permitted by law. Nothing in this Policy limits any legal right or remedy available to an individual.

24. Changes to This Policy

We may update this Policy to reflect changes in applicable law, our services, technology, security arrangements or data processing practices. The latest version will be published on <https://mydreamcv.com> with its effective or last-updated date.

Where a change materially affects individuals' rights or the purposes for which their personal data is processed, we will provide additional notice or obtain consent where required by law. Continued use of the website does not replace consent where consent is legally required.