XALCO LIMITED

Ujuzi Fursa Africa – Data Use and Privacy Policy

Effective Date: 10-04-2026
Last Updated: 10-04-2026

1. Who We Are

Xalco Ltd and Ujuzi Fursa Africa Training Institutes, operated by [full legal entity name] ("Ujuzi Fursa Africa," "we," "our," or "us"), is committed to protecting the privacy and personal data of our students, applicants, parents or guardians, website visitors, social media followers, staff, partners, and members of the public who interact with us.

This Policy explains how we collect, use, store, share, and protect personal data through our websites, social media pages, online forms, physical forms, admissions processes, training delivery, certification processes, student support activities, and related services. Our processing is guided by the principles of lawful, fair and transparent processing, purpose limitation, data minimization, accuracy, retention control, and appropriate safeguards.

2. Scope of This Policy

This Policy applies to personal data collected through:

- our websites and landing pages;
- our Facebook, Instagram, LinkedIn, TikTok, YouTube, WhatsApp, and other social media pages or channels;
- enquiry forms, scholarship forms, event registration forms, career interest forms, and lead-generation campaigns;
- student application, admission, enrolment, learning, certification, internship, attachment, placement, alumni, and support processes;
- phone calls, emails, chats, and in-person visits; and
- any other platform or tool used by Ujuzi Fursa Africa to collect or process personal data.

3. The Personal Data We May Collect

Depending on how you interact with us, we may collect the following categories of personal data:

A. Website & Social Media Data

- full name;
- phone number;
- email address;
- county, town, or location;
- course interest and study preferences;
- messages, comments, chat history, or enquiry details;
- device, browser, IP address, cookies, and usage data from our websites;
- marketing preferences; and
- photographs, videos, testimonials, or user-generated content where submitted to us or where you have consented.

B. Student & Applicant Data

- full name, date of birth, gender, nationality, and identification details;

- passport photo and identification documents;
- contact details and address;
- parent/guardian and next-of-kin details where applicable;
- academic history, certificates, transcripts, and references;
- application and interview records;
- course registration and attendance records;
- assessment, examination, practical, and certification records;
- fee, billing, scholarship, sponsorship, and payment information;
- internship, attachment, job-readiness, and placement-related information;
- disciplinary, welfare, safeguarding, accommodation, or support records where necessary; and
- limited health or disability information where required for reasonable accommodation, student safety, insurance, or legal compliance.

> ⚠ **SENSITIVE PERSONAL DATA**
>
> Where we collect sensitive personal data — such as health information, biometric data, family details, or children's data — we will only do so where necessary, lawful, and with appropriate additional safeguards. Kenya's framework treats sensitive and children's data with extra protection.

4. How We Use Personal Data

We may use personal data to:

- respond to enquiries and provide information about our courses, campuses, scholarships, events, and services;
- process applications, admissions, interviews, and enrolment;
- deliver education, training, assessments, examinations, and certification;
- maintain student records and academic administration;
- provide student welfare, safety, support, and reasonable accommodation;
- process payments, invoices, refunds, and financial records;
- communicate timetables, notices, updates, and operational messages;
- facilitate internships, attachments, industrial placements, alumni engagement, and employability initiatives;
- comply with legal, regulatory, accreditation, and reporting obligations;
- improve our websites, advertising, services, student experience, and operational performance;
- send marketing or promotional communications where permitted by law; and
- protect our institution, students, staff, systems, and the public against fraud, misuse, security incidents, or unlawful activity.

5. Our Legal Bases for Processing

We process personal data on one or more of the following lawful bases:

Lawful Basis	When We Rely On It
Consent	You have clearly agreed to a specific use.
Pre-contractual / Contract	Processing an application, enrolment, training, or related student service.
Legal Obligation	Keeping records or disclosing information under applicable law, regulations, or accreditation obligations.
Vital Interests	Processing necessary to protect someone's life, health, or safety.
Legitimate Interests	A reasonable business or institutional need not overridden by data subject rights.

6. Marketing, Social Media, Photos & Testimonials

We may use contact information to send course updates, admissions information, event invitations, scholarship opportunities, alumni news, or other promotional messages where permitted by law. You may opt out of direct marketing at any time.

If you contact us through social media or messaging apps, the platform provider may also process your information under its own privacy policy. We encourage users not to post sensitive personal data publicly in comments, captions, or open chats.

We may publish photographs, videos, student success stories, testimonials, or event content on our websites, brochures, and social media pages only where we have an appropriate lawful basis.

CHILDREN IN PHOTOS

Where content relates to a child or minor, we will seek consent from a parent or legal guardian before public use. The ODPC's education guidance specifically requires parental or guardian consent before publishing or sharing children's photographs in public domains.

7. Children and Minors

Where an applicant or student is a minor, we may collect and process their data through a parent or legal guardian and may require proof of that parent's or guardian's authority. We may also implement age checks, consent forms, and additional child-protection controls where appropriate.

The ODPC's education guidance states that minors cannot validly give consent on their own for these purposes, and that parental or guardian consent and verification of authority are required before collecting or processing children's data.

8. Sharing of Personal Data

We may share personal data only where necessary and appropriate with:

- our authorized staff and management on a need-to-know basis;
- affiliated campuses or business units within our organization where relevant to service delivery;
- payment processors, cloud providers, CRM systems, website hosts, analytics providers, email or SMS service providers, and other contracted service providers;
- accrediting, examining, certifying, internship, or placement partners where required for student progression or opportunity pathways;
- professional advisers, auditors, insurers, and legal counsel;
- government bodies, regulators, law-enforcement agencies, or courts where required by law; and
- any other party where the data subject has consented or where disclosure is otherwise lawful.

Where we use third-party processors, we expect them to protect personal data, act only on documented instructions, and apply appropriate security and confidentiality safeguards.

9. International Transfers

Some of our service providers or digital platforms may store or process personal data outside Kenya. Where this happens, we will take reasonable steps to ensure that the transfer is lawful and that appropriate safeguards are in place. Where sensitive personal data is transferred outside Kenya, we will apply the additional safeguards required by law.

10. Data Retention

We will keep personal data only for as long as necessary for the purpose for which it was collected, or as required by law, regulation, accreditation, audit, dispute resolution, safeguarding, or legitimate institutional record-keeping needs.

Our retention periods may differ depending on the category of data. For example, we may keep enquiry records for a shorter period than enrolled-student academic records or legally required financial records. Where data is no longer needed, we will securely delete, destroy, anonymise, or archive it in line with our retention schedule.

11. Data Accuracy

We take reasonable steps to keep personal data accurate and up to date. Students, applicants, parents, guardians, and other data subjects should notify us promptly if their details change or if they believe any information we hold is inaccurate, incomplete, outdated, or misleading.

12. Security Measures

We use reasonable technical and organizational measures to protect personal data against unauthorized access, loss, misuse, alteration, disclosure, or destruction. These measures may

include access controls, staff confidentiality obligations, password protection, secure storage, restricted user permissions, backups, and vendor due diligence.

DATA BREACH NOTIFICATION

Where a personal data breach creates a real risk of harm, Kenyan law requires notification to the Data Commissioner within 72 hours of awareness, and communication to affected data subjects within a reasonably practical period.

13. Cookies & Website Analytics

Our websites may use cookies, pixels, tags, and similar technologies to:

- keep the website working properly;
- understand website traffic and usage patterns;
- improve user experience;
- measure campaign performance; and
- support advertising and remarketing.

Where required, we will provide notice and request appropriate consent for non-essential cookies or tracking tools. Users can also manage cookies through their browser settings, though some website features may not function properly if cookies are disabled.

14. Your Rights

Subject to applicable law, a data subject has the right to:

- be informed of the use to which their personal data is put;
- access personal data in our custody;
- object to the processing of all or part of their personal data;
- request correction of false, misleading, inaccurate, incomplete, or outdated data; and
- request deletion or erasure in appropriate circumstances.

To exercise your rights, please contact us using the details below. We may ask for reasonable proof of identity before acting on a request.

15. Contact for Privacy Matters

For any privacy, data use, access, correction, deletion, objection, or complaint request, please contact:

DATA PROTECTION OFFICER

Privacy Contact / Data Protection Officer

Ujuzi Fursa Africa Training Institutes

Email: info@ujuzifursaafrica.ac.ke

16. Complaints

If you are dissatisfied with how we handle your personal data or a rights request, please contact us first so that we can try to resolve the issue. You also have the right to lodge a complaint with the Office of the Data Protection Commissioner (ODPC). The ODPC publishes data-subject rights, complaint channels, and Kenya's applicable data-protection regulations on its official website.

17. Changes to This Policy

We may update this Policy from time to time to reflect legal, operational, technological, or institutional changes. The latest version will be posted on our website with the revised effective date.