IDCL Privacy Policy

Nov 14, 2026 · @Prime

1. This policy explains how we collect, use, share and protect personal data. It applies to:

- our website imodigitalcity.com
- our training and talent programmes, including SkillUp Imo, IDCL bootcamps, the Summer Tech Bootcamp for children, and the talent placement service
- our startup programmes, including the Founder Dojo and the IDCL Founders Development Program run with the US Market Access Center (USMAC)
- our hubs and facilities, including the Digital Learning Centres, BPO and Call Centre, Auto Service Centre, Digital Printing Press and event spaces
- the government digital services we build and operate, such as staff and teacher verification, market enumeration, transport registration and digital payments

IDCL is the data controller for personal data processed for its own purposes. Where we process data on behalf of a Ministry, Department or Agency (MDA) of the Imo State Government, we act as data processor, or as joint controller with that MDA, depending on the arrangement. We comply with the Nigeria Data Protection Act 2023 (NDPA) and regulations and guidance issued by the Nigeria Data Protection Commission (NDPC).

Controller details

- Name: Imo Digital City Limited
- Address: 23 Egbu Road, Owerri, Imo State, Nigeria
- General enquiries: info@imodigitalcity.com

2. What we collect and why

We collect only the data each service needs. We collect it directly from you, from the MDA that engaged us for a programme, or automatically when you use our websites and platforms.

Category	Examples	Why we use it	Lawful basis (NDPA s.25)
Identity and contact	Name, gender, date of birth, phone, email, address, LGA and state of origin, photograph	Registration, verification and communication across all services	Contract; public interest task; consent
Website enquiries and bookings	Contact form messages, appointment requests and purpose of visit, partner and employer requests	Responding to you and scheduling visits to our campus	Legitimate interest; steps before a contract

Category	Examples	Why we use it	Lawful basis (NDPA s.25)
Newsletter subscribers	Email address, marketing preferences	Sending updates you asked for	Consent
Training and bootcamp participants	Course choice, attendance, assessments, certificates, fee payment receipts	Delivering training and issuing certificates	Contract
Talent candidates	CV, skills, assessment results, location, placement and performance feedback	Matching candidates to employers and tracking placements	Contract; consent before profiles are shared with an employer
Founders and startups	Founder names, contact details, startup information, pitch materials, bootcamp and selection results	Selecting, mentoring and accelerating startups and connecting them with investors	Contract; consent
Event registrants	Name, contact details, organisation, showcase interest	Managing registration and attendance	Contract; consent
Facility customers	Auto Service Centre vehicle and owner details, printing orders, event space bookings	Providing the service and billing	Contract
Government identifiers	NIN, BVN, staff, teacher or file numbers	Verifying identity and eligibility for government programmes	Legal obligation; public interest task
Financial	Bank name, account number, account name, transaction records	Payroll validation, payments, revenue collection and reconciliation	Contract; legal obligation
Employment and education	Employer, role, posting, qualifications, certificates	Staff and teacher verification	Public interest task
Business and transport	Business name, trade category, shop or stall location, vehicle and route details	Market enumeration and transport registration	Public interest task
Biometric (sensitive)	Fingerprints used for matching	Preventing impersonation and duplicate enrolment in verification exercises	Explicit consent or substantial public interest

Category	Examples	Why we use it	Lawful basis (NDPA s.25)
			under law (NDPA s.30)
Photos, video and recordings	Event and class photos, livestreams, testimonials, call recordings at the BPO and Call Centre where used	Publicity, quality assurance and training	Consent; legitimate interest for quality assurance with notice
Technical	IP address, device and browser data, log-in records, cookies	Security, fraud prevention and service improvement	Legitimate interest; consent for non-essential cookies
Visitor and CCTV	Visitor logs, CCTV footage at IDCL premises	Physical security of people and equipment	Legitimate interest

We process sensitive personal data, including biometrics, only where the NDPA permits and with additional safeguards. We do not make decisions about you based solely on automated processing that produce legal or similarly significant effects without human review.

If you do not provide data that a service requires, we may be unable to register, verify or pay you for that service.

3. Children's data

Some of our programmes, such as the Summer Tech Bootcamp for ages 9 to 16, involve children. Under section 31 of the NDPA, we process a child's personal data only with the consent of a parent or legal guardian, and we take reasonable steps to verify that consent.

- A parent or guardian completes registration and gives consent on the child's behalf.
- We collect only what we need: the child's name, age, school, track choice, any support needs the parent chooses to tell us about, and the parent's contact details.
- We do not use children's data for marketing, profiling or advertising.
- Photos, videos, testimonials or a child's name are published only with the parent's separate, specific consent, which can be withdrawn at any time. Testimonials use first names only.
- Parents can ask to see, correct or delete their child's data at any time.

4. Photos, recordings and livestreams

We take photos and video at classes, bootcamps, hackathons and events, and some events are livestreamed on Facebook and YouTube. We tell attendees in the registration details and at the venue when this happens.

If you do not want to appear in photos or a livestream, tell the organiser or our team at the event and we will avoid or remove footage of you where we reasonably can. Testimonials and quotes are published only with the person's agreement.

Where the BPO and Call Centre records calls, callers are told at the start of the call.

5. Sharing, transfers, retention and security

Who we share with. We do not sell personal data. We share it only as needed with:

- Imo State Government MDAs that commissioned a programme or are responsible for the service
- Programme partners, such as the US Market Access Center (USMAC) for the Founder Dojo and Founders Development Program, and training partners for SkillUp Imo, only for the programme you joined
- Employers, when you are a talent candidate, but only after you agree to your profile being shared
- Mentors and investors, when you are a founder in one of our startup programmes, limited to your startup information and pitch materials
- Service providers acting on our instructions, such as cloud hosting, email, payment and bank verification providers, and software partners, under written contracts that bind them to the NDPA
- Banks and payment processors, to complete payments you request or are owed
- Social media platforms, such as Facebook and YouTube, when an event you attend is livestreamed
- Regulators, courts and law enforcement, where the law requires it

How long we keep it. We keep personal data only as long as the purpose requires, or as long as the law or the commissioning MDA requires. Retention periods are set out in the IDCL Data Retention Policy. When data is no longer needed, we delete it securely or anonymise it.

How we protect it. We use technical and organisational measures appropriate to the risk, including:

- Encryption in transit (HTTPS/TLS) and at rest through our hosting providers
- Role-based access control, strong authentication and least-privilege access
- Audit trails and activity logs on our platforms
- Regular backups and recovery procedures
- Firewalls and network security controls
- Staff confidentiality obligations and data protection training
- A breach response procedure. Where a breach is likely to risk your rights, we notify NDPC within 72 hours, and notify you without undue delay where the risk is high.

6. Your rights

Under the NDPA you have the right to:

- Be informed about how your data is used
- Access the personal data we hold about you and receive a copy
- Have inaccurate or incomplete data corrected

- Have your data erased where there is no longer a lawful reason to keep it
- Restrict or object to processing, including processing for direct marketing
- Receive your data in a portable format where processing is based on consent or contract
- Withdraw consent at any time, without affecting processing already carried out
- Not be subject to a decision based solely on automated processing that significantly affects you

To exercise a right, contact us by email. We may ask you to verify your identity. We respond within 30 days. Some rights are limited where we process data for a public interest task or to meet a legal obligation; we will explain if that applies.

7. Newsletters and cookies

We send newsletters and programme updates only to people who opt in, for example by ticking the marketing box on our newsletter form. Every email includes an unsubscribe link, and you can also opt out by emailing info@imodigitalcity.com.

Our websites use essential cookies to keep them secure and working. We use analytics or other non-essential cookies only with your consent, which you can give or withdraw through the cookie banner or your browser settings.

8. Complaints

If you have a concern, contactus by email info@imodigitalcity.com. We acknowledge complaints within 5 working days and aim to resolve them within 30 days.

9. Changes to this policy

We review this policy at least once a year and when our processing changes. The current version is always published on our website with its effective date.