



# **SPEEDLINK INSTITUTE OF TECHNOLOGY AND INNOVATIONS (SITI)**

Policy and Procedure: Learner Registration and Administration

Policy Number: SITI-ADM-LRA-001

Version: 1.0

Effective Date: 1st, February 2026

Approved By: SITI Board of Directors

# 1. Purpose

To establish a clear, efficient, and secure process for:

- Registering and enrolling all learners into SITl programs.
- Collecting, verifying, and storing student documentation.
- Issuing student identification cards and LMS credentials.
- Maintaining accurate, confidential student records throughout the learner lifecycle (from admission to post-graduation).
- Ensuring compliance with data protection principles and audit requirements.

This policy supports SITl's core values of Integrity (accurate records) and Excellence (efficient administration).

# 2. Scope

This policy applies to:

- All learners enrolled in any SITl training pathway: Individual Training, Corporate Training, Partner/Donor-supported initiatives, NYSC, SIWES.
- All administrative staff responsible for registration, documentation, ID cards, and record-keeping.
- The Training Coordinator for oversight and exception handling.
- The Technical Team for LMS account creation and access management.
- All student records (physical and electronic) from initial inquiry through to post-graduation retention and eventual secure disposal.

This policy does not cover academic assessment records (covered under Assessment Procedure) or financial transactions (covered under separate Finance Policy, to be developed).

# 3. Definitions

---

Term	Definition
Applicant	A person who has expressed interest in a SITl program but has not yet completed enrollment.

---

Enrolment	The formal process by which an applicant becomes a registered student after completing all requirements (form, payment or scholarship approval, document submission).
Student Master File	The primary physical or electronic folder containing all documents related to a student's journey at SITl.
Student Identification (ID) Card	An official SITl-issued card bearing the student's name, photo, program, cohort, and a unique student number.
LMS Credentials	Username and password (or SSO) granting access to SITl's Learning Management System.
Cohort	A group of students who start a program together on the same start date.
Withdrawal	A student's formal exit from a program before completion.
Deferral	A student's approved postponement of their studies to a later cohort.

## Institute of Technology and Innovation

### 4. Policy Statement

SITl is committed to:

1. Accuracy: All student data entered into SITl systems will be complete, correct, and verified.
2. Confidentiality: Student personal information will be accessible only to authorised staff on a need-to-know basis.
3. Timeliness: Registration and access credentials will be provided before the first day of training.

4. Compliance: SITI will adhere to Nigerian data protection principles (as per NDPR 2019) and any partner requirements (e.g., EC-Council).
5. Record Integrity: Student master files will be maintained with both physical and cloud backups (per main SOP Section 4.2.1).

## 5. Registration and Enrollment Procedures

### 5.1 Pre-Enrollment (Applicant Stage)

Step	Action	Responsible	Timeline
1	Applicant expresses interest via website, email, phone, or in-person visit.	Marketing / Admin	Within 1 working day – send program information and enrollment form.
2	Applicant submits completed SITI Enrollment Form (Appendix A) along with required documents (see Section 5.2).	Applicant	At least 14 days before program start (late applications accepted at Coordinator's discretion).
3	Admin acknowledges receipt and checks form completeness.	Admin	Within 3 working days.
4	If incomplete, Admin requests missing information; applicant has 7 working days to provide.	Admin	–

### 5.2 Required Documents for Enrollment

All enrolling students must provide:

- Completed and signed Enrollment Form (Appendix A).
- Valid government-issued identification (National ID Number (NIN) card, Driver's Licence, International Passport, Voter's Card, or Local Government Certificate of Origin – as listed in main SOP Section 4.2.1).
- Passport-photograph (digital, for ID card and LMS profile).
- Evidence of payment (receipt of tuition or scholarship award letter from SITI). For scholarship students, the Training Coordinator confirms award before enrollment.
- Additional documents for special cases:
  - NYSC/SIWES students: Letter from institution or NYSC posting letter.
  - Corporate sponsored students: Sponsorship letter from employer.

Verification: Admin must verify the authenticity of government ID (compare photo, check for obvious forgery). For scholarship laptop provision (per Section 4.2.3 of main SOP), the ID is required before device handover.

### 5.3 Formal Enrollment and Record Creation

Once all documents are verified and payment/scholarship is confirmed, Admin completes the enrollment process:

Step	Action	Responsible	Timeline
1	Assign a unique Student ID Number (format: SITI/[Year]/[Cohort Code]/[Sequential Number], e.g., SITI/2026/APR/042).	Admin	Within 2 working days of document verification.
2	Create a Student Master File (physical folder and cloud folder).	Admin	Within 2 working days.

3	Enter student data into SITI's Student Database (spreadsheet or LMS-based).	Admin	Within 2 working days.
4	Request LMS account creation from Technical Team.	Admin	Same day as database entry.
5	Technical Team creates LMS account (username: student ID number, initial password generated securely).	Technical Team	Within 2 working days of request.
6	Admin notifies student of successful enrollment and provides LMS credentials (via email and WhatsApp, separately – password not sent via WhatsApp).	Admin	Within 1 working day of LMS account creation.
7	Schedule student for ID card capture (see Section 6).	Admin	Before orientation.

Student Master File contents (physical and cloud):

- Signed enrollment form.
- Copy of government ID.
- Passport photograph (printed for physical file, digital for LMS/ID).
- Proof of payment or scholarship award letter.
- LMS account confirmation.
- Attendance logs (added during program).
- Assessment records (added after grading, per Assessment Procedure).
- Certificate copy (added after graduation).

- Any correspondence related to deferral, withdrawal, or disciplinary action.

## 5.4 Orientation and Final Verification

At the mandatory orientation (per main SOP Section 4.2.2), Admin staff:

- Verify identity of each student by comparing government ID to the person (for ID card issuance – see Section 6).
- Collect any missing documents.
- Confirm LMS access on the student’s own device.
- Distribute printed orientation materials.

Consequence of non-attendance: Students who miss orientation without prior approval may have their enrollment cancelled or deferred to the next cohort.

## 6. Student Identification (ID) Card

### 6.1 Card Specifications

SITI issues a physical ID card to every enrolled student. The card includes:

- Student’s full name.
- Student ID number.
- Program name and cohort.
- Passport photograph.
- SITI logo.
- Issue date and expiry date (end of program + 3 months).
- Signature of Training Coordinator (or stamped).

Institute of Technology and Innovation

### 6.2 Issuance Process

Step	Action	Responsible
1	During orientation, Admin captures student’s photograph (or uses uploaded digital photo).	Admin

2	Admin designs card using template.	Admin
3	Admin prints card (using ID card printer or laminated paper card).	Admin
4	Student signs card (if applicable) and receives it at orientation or within first week.	Admin
5	Admin records ID card number (if sequential) in student master file.	Admin

Cost: The first ID card is free. Replacement for lost/damaged cards costs ₱2,000 (or as determined by SITI Board).

### 6.3 Use and Replacement

- Students must present their SITI ID card for:
  - Entry into SITI facilities or events (Graduation Week, Motivate & Connect, exams).
  - Certificate collection.
  - Access to scholarship laptops (if applicable).
- Lost cards must be reported to Admin immediately. Replacement requires payment of fee and a police report (if theft).
- Damaged cards (wear and tear) are replaced free of charge upon return of the damaged card.

## 7. LMS Account Administration

### 7.1 Account Creation and Access

- Technical Team creates LMS accounts using the Student ID Number as the username.
- Initial password is generated securely (e.g., random alphanumeric) and sent to the student's registered email (not via WhatsApp).
- Students must change their password on first login.
- Each student's LMS profile includes: full name, student ID, program, cohort, and enrollment status (active, withdrawn, graduated).

## 7.2 Account Maintenance

Event	Action	Responsible
Student requests password reset	Verify identity, then reset password via LMS “forgot password” function or manually.	Technical Team (within 1 working day).
Student changes email or phone number	Student notifies Admin; Admin updates student master file and LMS profile.	Admin (within 2 working days).
Student withdraws or defers	Admin changes LMS status to “inactive” or “deferred”; removes access to course content (except archived materials).	Admin + Technical Team.
Student graduates	LMS status set to “alumni”; retains access to archived materials for 1 year (optional).	Technical Team.

## 7.3 Security and Data Protection

- LMS access logs are retained for 12 months.
- Students must not share their passwords. Sharing credentials is a violation of the Student Code of Conduct and may result in disciplinary action.
- Technical Team ensures LMS is hosted on a secure platform with encryption and regular backups.

## 8. Changes to Student Status

### 8.1 Program Transfer (Within SITI)

A student may request to transfer from one program to another (e.g., from Web Development to Cybersecurity) before the end of the second week of the program.

Procedure:

1. Student submits written request to Training Coordinator.
2. Coordinator assesses eligibility (e.g., prerequisites, space availability).
3. If approved, Admin updates student master file, LMS enrollment, and issues a new ID card (no fee for first transfer).
4. Tuition difference (if any) is paid or refunded per Finance Policy.

## 8.2 Deferral

A student may request to defer their studies to a later cohort for valid reasons (medical, family emergency, national service).

Procedure:

1. Student submits written request with supporting evidence to Training Coordinator.
2. Coordinator approves deferral for up to two consecutive cohorts (maximum 12 months).
3. Admin changes student status to “Deferred” in LMS and master file.
4. Tuition paid is carried forward to the new cohort. No additional tuition is charged unless the program curriculum has changed significantly (then pro-rated adjustment may apply).
5. After two deferrals without re-enrollment, the student is considered withdrawn, and tuition is forfeited.

## 8.3 Withdrawal

A student may withdraw from a program voluntarily. Withdrawal is effective from the date SITI receives written notice.

Procedure:

1. Student submits written withdrawal notice to Admin.
2. Admin calculates refund (if any) per SITI Refund Policy (to be developed – typically: 100% before orientation, 50% before week 3, 0% after).
3. Admin closes LMS access (or sets to “withdrawn” read-only).
4. Admin updates master file and database.
5. Student returns ID card (if possible).

Involuntary withdrawal (expulsion): Occurs only after a disciplinary process under Malpractice Policy or Grievance Policy. The student is notified in writing, and no refund is given.

## 8.4 Reinstatement

A student who withdrew or was expelled may apply for reinstatement to a future cohort. Reinstatement is at the sole discretion of the Training Coordinator and may require re-application and full tuition payment.

## 9. Record Keeping and Data Management

### 9.1 Storage and Backup

Per main SOP Section 4.2.1, Admin maintains:

- Physical student master files in a locked filing cabinet, accessible only to Admin staff and Training Coordinator.
- Cloud backups (encrypted) of all student documents, updated weekly.

### 9.2 Retention and Disposal

Per main SOP Section 5.1:

Record Type	Retention Period	Disposal Method
Student master files (all documents)	5 years post-graduation or withdrawal	Shredding (physical) / secure deletion (digital).
LMS user data (including grades)	3 years post-graduation (or longer if required by partner)	Anonymised export then deletion.
ID card issue records	3 years	Shredding.
Withdrawal and deferral requests	3 years after final action	Secure deletion.

Before disposal, Admin must obtain written approval from the Training Coordinator.

### **9.3 Data Protection and Confidentiality**

- Student personal data (ID copies, phone numbers, addresses) will not be shared with third parties except:
  - As required by law (e.g., law enforcement subpoena).
  - With the student's written consent.
  - For legitimate SITI purposes (e.g., sharing attendance data with a scholarship donor) with appropriate confidentiality agreements.
- All staff with access to student records must sign a Confidentiality Agreement (Appendix B).
- Any data breach (unauthorised access, loss of records) must be reported to the Training Coordinator within 24 hours and to the Board within 72 hours.

### **9.4 Student Access to Own Records**

A current or former student may request access to their own student master file. Admin must provide a copy (physical or digital) within 10 working days of a written request. A reasonable fee may be charged for extensive photocopying.

## **10. Registration Reports and Statistics**

The Training Coordinator includes in the monthly report to the Board (per main SOP Section 5.2):

- Total enrolled students (by program, cohort, gender, scholarship status).
- New registrations (since last report).
- Withdrawals, deferrals, and transfers.
- ID cards issued and replacements.
- Any data protection incidents or record-keeping issues.

An annual registration summary is produced for internal audit and external partners (e.g., EC-Council may require enrollment numbers).

## **11. Roles and Responsibilities**

Role	Registration & Administration Responsibilities
Admin Staff	Collect and verify documents; create student master files; issue ID cards; maintain database; process status changes; ensure data accuracy and confidentiality.
Training Coordinator	Oversee registration process; approve deferrals, transfers, and reinstatements; report to Board; act as data protection officer (interim).
Technical Team	Create and manage LMS accounts; ensure secure access; assist with password resets.
Marketing Team	Forward inquiries and enrollment forms to Admin; collect graduate outcomes data for alumni records.
All Staff	Report any data security concerns or discrepancies in student records to Admin immediately.

## 12. Related Documents and Policies

- SITI Comprehensive SOP (Version 2.0, April 2026) – Sections 4.2, 4.1.3, 5.1.
- SITI Data Protection and Privacy Policy (to be developed – this policy provides interim guidance).
- SITI Equal Opportunity and Diversity Policy (for non-discrimination in registration).
- SITI Assessment Procedure (for grade records).
- SITI Refund Policy (to be developed – for withdrawal refunds).
- Nigerian Data Protection Regulation (NDPR) 2019.

## 13. Policy Review

This Learner Registration and Administration Policy will be reviewed biannually as part of SITI's SOP review cycle (Section 5.3 of main SOP) or whenever there is a significant change in data protection law or SITI's enrollment systems.

# Appendix A: SITI Student Enrollment Form

(To be provided to applicants – digital or paper)

Field	Information
Program Applying For	<input type="checkbox"/> Web Development <input type="checkbox"/> Cybersecurity <input type="checkbox"/> Data Science <input type="checkbox"/> Digital Marketing <input type="checkbox"/> Entrepreneurship <input type="checkbox"/> Other: _____
Cohort Start Date	
Personal Details	
Full Name (as on ID)	
Date of Birth	
Gender	<input type="checkbox"/> Male <input type="checkbox"/> Female <input type="checkbox"/> Prefer not to say
Address	
Email	
Phone Number (WhatsApp)	
Education / Background (optional)	Highest qualification: _____
How did you hear about SITI?	<input type="checkbox"/> Social media <input type="checkbox"/> Friend <input type="checkbox"/> Radio <input type="checkbox"/> Event <input type="checkbox"/> Other: _____
Sponsorship	<input type="checkbox"/> Self-sponsored <input type="checkbox"/> Employer (name: _____) <input type="checkbox"/> Scholarship (name: _____)
Emergency Contact	Name: _____ Phone: _____ Relationship: _____

---

Declaration: I confirm that the information provided is true and complete. I have read and understood SITI's policies (available at [www.speedlinkinstitute.org/policies](http://www.speedlinkinstitute.org/policies)). I consent to SITI processing my personal data for registration, training, and certification purposes.

---

Signature

---

Date

---

For Office Use:

- Received by: \_\_\_\_\_ Date: \_\_\_\_\_
  - Documents verified:  Yes (ID type: \_\_\_\_\_)  Pending
  - Payment/scholarship confirmed:  Yes  No
  - Student ID assigned: \_\_\_\_\_
  - LMS account created:  Yes (date: \_\_\_\_\_)
  - ID card issued:  Yes (date: \_\_\_\_\_)
  - Master file created:  Physical  Cloud
- 

## Appendix B: Staff Confidentiality Agreement (Student Records)

I, the undersigned, acknowledge that in the course of my duties at SITI, I may have access to student personal data, including identification documents, contact details, academic records, and financial information. I agree to:

1. Access student records only when necessary for my legitimate job functions.
2. Not disclose any student information to unauthorised persons (including family, friends, or social media).
3. Not remove physical student files from the Admin office without written authorisation.
4. Use strong passwords for any systems containing student data and not share my login credentials.
5. Immediately report any actual or suspected data breach to the Training Coordinator.

6. Return all student records and access credentials upon termination of my engagement with SITI.

I understand that violation of this agreement may result in disciplinary action, up to and including termination of employment or contract, and may lead to legal liability under Nigerian data protection law.

Name: \_\_\_\_\_ Role: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Witness (Training Coordinator): \_\_\_\_\_ Date: \_\_\_\_\_



# SPEEDLINK

---

Institute of Technology and Innovation

---