MASDAR CYBER

ComplianceIQ Africa

Compliance Assessment Report (Sample)

NDPA 2023 and ISO/IEC 27001:2022 gap assessment

Organisation	Acad School (fictitious organisation)
Industry / sector	Education and EdTech
Size	Micro (1–9 staff)
Assessment date	27 October 2026
Report reference	MC-SAMPLE-01
Report version	1.0
Prepared by	Quadri Durodola, Founder and Principal Consultant, Masdar Cyber Ltd
Classification	SAMPLE: for illustration only

SAMPLE REPORT. Acad School is a fictitious organisation. This sample shows the format and depth of a ComplianceIQ Africa assessment; it is not advice for any real organisation. A real report is confidential to the client and is based on that client's own answers.

1. Executive summary

NDPA 2023	ISO/IEC 27001:2022	OVERALL RISK LEVEL
22%	**25%**	**Critical**
readiness on questions assessed	readiness on questions assessed	3 of 7 risks rated Critical

Acad School is a micro educational institution that processes employee HR records and children's data. On the answers provided, it scores 22% for NDPA 2023 readiness and 25% for ISO/IEC 27001:2022 readiness (Section 3 explains how the scores are calculated). The most significant gaps are the absence of a documented lawful basis for any processing, the lack of a parental consent process for uses of children's data beyond education, and incomplete technical security measures on staff devices. Three of the seven risks in Section 5 are rated Critical.

The immediate priority, within 30 days, is to record what personal data the school processes and on what lawful basis, to introduce parental consent for non-educational uses, and to put baseline device security in place. A data privacy impact assessment for pupil records should follow in Phase 2.

2. Scope, method and limitations

Scope

The assessment covers the Nigeria Data Protection Act 2023 (NDPA), with reference to the NDPA General Application and Implementation Directive 2025 (GAID) where relevant, and selected requirements of ISO/IEC 27001:2022, drawn from its management-system clauses (Clauses 4 to 10) and Annex A controls, as covered by the questionnaire. It is not a full ISO/IEC 27001 audit.

Method

Acad School completed the ComplianceIQ Africa questionnaire. Its answers were analysed using the ComplianceIQ Africa methodology, which is AI-assisted. The resulting draft was then checked, corrected where needed and approved by a consultant under Masdar Cyber Ltd's documented AI Output Review Procedure before delivery.

Limitations

- The findings rest entirely on the answers provided. Masdar Cyber Ltd has not independently verified them.
- This report is a pre-audit readiness evaluation. It is not an audit, a certification or a statement that the organisation is compliant, and it does not constitute legal advice.
- It reflects the position on the assessment date. Changes to the organisation, its processing or the law after that date are not reflected.

3. How to read this report

Readiness scores

Each question carries a weight of 2 or 3, reflecting its importance. A “Yes” answer earns the full weight, “Partial” earns half, and “No” earns nothing. Each score is the points earned as a percentage of the points available. NDPA and ISO/IEC 27001 results are reported separately, and the children’s data questions are not counted in either score. The weights reflect Masdar Cyber Ltd’s professional judgement, not a regulatory standard. A score shows readiness on the questions asked; it is not a measure of legal compliance.

Risk ratings

Each risk is scored for Likelihood (L) and Impact (I) from 1 (lowest) to 5 (highest). The risk score is L × I, which gives the rating below.

Score (L × I)	Rating	What it means
20–25	**Critical**	Address immediately; included in Phase 1 of the roadmap.
12–19	**High**	Address within the 90-day roadmap, usually Phase 1 or 2.
6–11	**Medium**	Plan within the roadmap or the following review cycle.
1–5	**Low**	Monitor; address as resources allow.

References

NDPA provisions are cited by Section (for example, NDPA s.24). GAID provisions are cited by Article. ISO/IEC 27001:2022 management-system requirements are cited as Clauses (for example, Clause 6.1.2) and controls as Annex A references (for example, A.5.34).

Priority phases

Each gap is assigned to a roadmap phase: Phase 1 (Days 1–30), Phase 2 (Days 31–60) or Phase 3 (Days 61–90).

4. Critical compliance gaps

The gaps below are the highest-priority exposures identified from the answers provided, each with the reference it rests on and the action recommended.

Gap 1: No documented lawful basis for any processing | Phase 1	
Framework	NDPA
Reference	NDPA s.25(1); s.24(3)
Finding	The school has not documented which lawful basis under Section 25(1) applies to each of its processing activities, including employee HR records and children's enrolment records.
Impact	Section 24(3) requires the school to demonstrate accountability for how it processes personal data. Without a documented lawful basis for each activity, it cannot show that its processing is lawful if a parent, an employee or the NDPC asks.
Recommended action	List each category of personal data the school processes (for example, employee HR records, enrolment records, academic records and parents' contact details) and record the lawful basis for each under Section 25(1). For example, employee HR records will usually rest on performance of the employment contract (s.25(1)(b)(i)). Keep this in a simple register of processing activities and have the principal approve it.

Gap 2: No parental consent process for uses of children's data beyond education | Phase 1	
Framework	NDPA
Reference	NDPA s.31(1)–(4); s.26
Finding	The school processes children's data and has no process for obtaining or verifying parental consent for uses beyond teaching, such as publishing pupils' photographs or sharing data with third-party platforms.
Impact	Section 31(4)(b) means parental consent is not required for processing carried out for education by a provider owing a duty of confidentiality. For other uses that rely on consent, Section 31(1) requires the consent of a parent or legal guardian, and Section 26(1) places the burden of proving that consent on the school.
Recommended action	Add a separate consent section to the enrolment form that lists each non-educational use (for example, photographs, newsletters, social media and named third-party tools), gives a separate yes or no choice for each, and explains how consent can be withdrawn. Confirm that consent comes from the parent or guardian using a proportionate check, such as the identity checks the school already carries out at enrolment; Section 31(3) recognises a government-approved ID as an appropriate mechanism. If an ID is sighted, record that it was seen rather than keeping a copy. Store signed forms securely.

Gap 3: Privacy notice incomplete | Phase 1	
Framework	NDPA
Reference	NDPA s.27(1), s.27(3)
Finding	The school's privacy notice is only partly in place.
Impact	Section 27(1) requires the school to tell people, before it collects their data, who it is and how to contact it, the lawful basis and purposes of processing, who receives the data, their rights, how long data is kept and their right to complain to the Commission. Section 27(3) requires this in a privacy policy that is clear and easily accessible for its audience: here, parents, pupils and staff.
Recommended action	Complete a plain-language privacy notice that covers each item in Section 27(1). Give it to parents at enrolment and to staff in the staff handbook, and publish it on any communications platform the school uses with parents.

Gap 4: Incomplete technical security controls on staff devices | Phase 1	
Framework	Both
Reference	NDPA s.39; ISO/IEC 27001:2022 A.8.5, A.8.7, A.8.24
Finding	Staff devices have no antivirus software, encryption of stored and transmitted data is not confirmed, and multi-factor authentication is in place on only some accounts.
Impact	Section 39(1) requires technical measures appropriate to the sensitivity of the data and the likely harm from its loss; Section 39(2)(b) names encryption as one such measure. Children's records and HR records held on unprotected devices are exposed to loss, theft and malware.
Recommended action	Install and keep up to date antivirus software on all staff devices (A.8.7). Turn on full-disk encryption on every device that stores personal data, and use HTTPS for any school website or portal (A.8.24). Enforce multi-factor authentication on all staff email and administrative accounts (A.8.5). Name one member of staff to oversee these controls.

Gap 5: No data privacy impact assessment (DPIA) process | Phase 2	
Framework	Both
Reference	NDPA s.28; GAID 2025 Art. 28(3)(e), 28(3)(m), 28(4), 28(10), 28(12); ISO/IEC 27001:2022 Clause 6.1.2, A.5.34
Finding	The school has no process for assessing privacy risks before introducing new processing activities, and has not carried out a DPIA for its existing processing of pupil records.
Impact	GAID 2025 Article 28(3) makes a DPIA mandatory, and requires it to be filed with the Commission, for educational services involving the processing of records relating to students or pupils. Article 28(4) requires the DPIA to be vetted by a DPO certified by the Commission. As a school processing children's records, Acad School's core processing appears to fall within Article 28(3)(m), and children are also vulnerable data subjects under Article 28(3)(e). Article 28(10) required a DPIA within six months of the GAID's issuance for processing that began before it, so this obligation is already overdue.
Recommended action	Complete a DPIA for the school's existing processing of pupil records, arrange for it to be vetted by a DPO certified by the Commission, and file it with the Commission; because the deadline has passed, begin arranging the DPO in Phase 1. Then introduce a short screening checklist to be completed before adopting any new tool, service or process involving personal data, with the principal as the sign-off.

Gap 6: No information security policy or assigned security responsibilities | Phase 1	
Framework	ISO 27001
Reference	ISO/IEC 27001:2022 Clauses 5.1, 5.2, 5.3; A.5.1, A.5.2
Finding	There is no written information security policy, no named person is responsible for information security, and leadership has not formally engaged with security governance.
Impact	Without a policy and an owner, other security controls lack direction and accountability, and staff have no clear basis for what is expected of them.
Recommended action	Draft a one-page information security policy suited to a micro organisation, covering acceptable use, data protection obligations, incident reporting and password requirements. Have the principal approve and sign it. Name a member of staff as information security owner, responsible for maintaining the controls and reviewing them annually.

5. Information security and data protection risk register

L = Likelihood (1–5). I = Impact (1–5). Score = L × I, rated as shown in Section 3.

ID	Risk statement	L	I	Score / rating	Recommended control
R001	Children's data is used beyond education, such as photographs and communications, without verified parental or guardian consent. (Current: no consent process.)	4	5	**20 Critical**	Separate consent section on the enrolment form for each non-educational use; parent or guardian confirmed by a proportionate check, such as a government-approved ID sighted; consents recorded and stored securely (NDPA s.31, s.26).
R002	No lawful basis is documented for any processing of employee HR records or children's enrolment records. (Current: none.)	5	4	**20 Critical**	Register of processing activities recording the lawful basis for each activity; reviewed annually (NDPA s.25(1), s.24(3)).
R003	Personal data on staff devices, including HR records and children's data, is unencrypted and unprotected by antivirus software, exposing it to loss, theft or malware. (Current: multi-factor authentication on some accounts only.)	4	5	**20 Critical**	Antivirus on all staff devices; full-disk encryption on devices holding personal data; multi-factor authentication on all email and administrative accounts (NDPA s.39; A.8.7, A.8.24, A.8.5).
R004	A personal data breach involving children's or employee data may not be reported to the NDPC within the 72 hours required by NDPA s.40(2). (Current: partial procedure, not documented or tested.)	3	5	**15 High**	Written breach response procedure naming the responsible person, the 72-hour notification step and a notification template; breach log (s.40(8)); annual tabletop test (NDPA s.40; A.5.24–A.5.26).
R005	Staff handling children's data and HR records have had no documented data protection or security awareness training, increasing the risk of accidental disclosure, mishandled consent or unrecognised incidents. (Current: none.)	4	4	**16 High**	Documented awareness training for all staff, repeated at least annually, with attendance records, under a written training schedule (NDPA s.24(2)–(3); GAID Art. 30; A.6.3).
R006	No DPIA has been carried out for the processing of pupil records, which GAID 2025 Article 28(3) makes mandatory for educational services. (Current: none.)	3	4	**12 High**	DPIA for pupil-record processing, vetted by a Commission-certified DPO and filed with the Commission; screening checklist for new processing (NDPA s.28; GAID Art. 28).
R007	There is no written information security policy and no one has assigned security responsibilities, leaving no basis to sustain or improve controls. (Current: none.)	5	3	**15 High**	Approved information security policy; named security owner; responsibilities communicated to all staff; annual review (Clauses 5.2, 5.3; A.5.1, A.5.2).

6. 90-day remediation roadmap

The roadmap is sequenced so the highest risks are addressed first and later phases build on earlier ones.

Phase 1 — Days 1–30: Foundation

1. Record each personal data processing activity (employee HR records, children's records and others) and its lawful basis under NDPA s.25(1) in a simple register of processing activities.
2. Add a parental consent section for non-educational uses of children's data to the enrolment form, with a proportionate check that consent comes from the parent or guardian, such as sighting a government-approved ID (NDPA s.31(2)–(3)).
3. Install antivirus software on all staff devices, turn on full-disk encryption on devices holding personal data, and enforce multi-factor authentication on all staff email and administrative accounts.
4. Draft a one-page information security policy, have the principal approve and sign it, and name a member of staff as information security owner.
5. Complete and publish a privacy notice that covers each item in NDPA s.27(1), and give it to staff, parents and guardians.

Phase 2 — Days 31–60: Implementation

1. Deliver documented data protection and security awareness training to all staff, covering children's data, consent, incident reporting and acceptable use of school systems, under a written training schedule with a basic privacy checklist for staff (GAID Art. 30); keep attendance records.
2. Write a step-by-step breach response procedure naming the responsible person, the 72-hour NDPC notification step (NDPA s.40(2)) and escalation; start a breach log (s.40(8)); walk through it with staff.
3. Complete a DPIA for the processing of pupil records, have it vetted by a Commission-certified DPO and file it with the Commission (GAID 2025 Art. 28); introduce a screening checklist for any new tool, service or process involving personal data.
4. Write a data retention and secure disposal policy setting how long each category of personal data is kept and how it is securely deleted (NDPA s.24(1)(d)).

Phase 3 — Days 61–90: Review and readiness

1. Carry out an internal review of the controls put in place in Phases 1 and 2, record the findings and assign a named owner to each open item (ISO/IEC 27001:2022 Clause 9.2).
2. Put written agreements in place with every third party that processes personal data for the school, such as cloud storage or payroll providers (NDPA s.29(2)).
3. Hold a leadership review of the information security and data protection programme, record the outcomes and actions, and schedule it annually (ISO/IEC 27001:2022 Clause 9.3).

7. Consultant's commentary

The low scores reflect missing decisions and paperwork more than any single failure. Most of what Acad School needs to do in Phase 1 involves writing down what the school already does, assigning responsibility to specific staff, and turning on standard security protections that are mostly free or low-cost.

Children's data is the centre of Acad School's data protection position. The law allows the school to process pupils' data for teaching without separate parental consent, but that does not extend to uses beyond education, such as publishing pupils' photographs on social media or sharing their data for other purposes. That is why the parental consent process in Gap 2 is essential. The school's main formal obligation is a Data Privacy Impact Assessment (DPIA) under GAID 2025 Article 28, which applies to educational services processing pupil records and to processing that involves children. Because this DPIA is already overdue, the school should begin arranging a Commission-certified DPO to vet it in Phase 1, and budget for that cost.

On information security, the school's gaps are about basic device protection rather than complex technical systems. Installing antivirus software, enabling full-disk encryption and enforcing multi-factor authentication will reduce the Critical device-security risk (R003) quickly. The other two Critical risks, on consent and lawful basis, are fixed through documentation and process rather than technology. Approving a simple one-page policy and naming a staff member to oversee security gives all of these protections proper ownership.

Acad School already has useful foundations to build on: multi-factor authentication on some accounts, a partial privacy notice and a partial breach procedure. Completing these existing pieces, rather than starting from scratch, makes this 90-day roadmap realistic for an organisation of its size.

8. Next steps

If Acad School would like support with the roadmap, Masdar Cyber Ltd can help with the following. Each is scoped and quoted separately.

Service	Description
Documentation support	Drafting the documents the roadmap calls for: privacy notice, parental consent form, register of processing activities, information security policy, breach response procedure and retention policy.
DPIA preparation	Preparing the DPIA for pupil-record processing, ready for vetting by a Commission-certified DPO.
Follow-up review	A review of progress against the roadmap after 90 days.

Quadri Durodola | Founder and Principal Consultant, Masdar Cyber Ltd | info@masdarcyber.com | masdarcyber.com

9. Review and approval

Draft produced with	ComplianceIQ Africa (AI-assisted)
Reviewed by	Quadri Durodola, Founder and Principal Consultant
Review standard	Masdar Cyber Ltd AI Output Review Procedure
Review outcome	Amend and approve
Date approved	_____
Report version	1.0

Legal disclaimer

This report is prepared by Masdar Cyber Ltd for advisory purposes only. It does not constitute legal advice and should not be relied on as a substitute for independent legal counsel. Findings are based on information provided by the organisation, which has not been independently verified. Masdar Cyber Ltd accepts no liability for decisions made solely on the basis of this report. Organisations required to file Compliance Audit Returns with the NDPC must do so through a licensed Data Protection Compliance Organisation (DPCO). This assessment is an independent pre-audit readiness evaluation and does not constitute an audit, a certification or a ForHumanity certified audit.