SCHOLANET TECHNOLOGIES

EDUCATION DATA GOVERNANCE, ANALYTICS & INFORMATION-SHARING FRAMEWORK

RESPONSIBLE EDUCATION DATA FOR BETTER PLANNING, BETTER DECISIONS & BETTER OUTCOMES

COLLECT RESPONSIBLY · PROTECT CAREFULLY · ANALYSE RESPONSIBLY · SHARE ONLY WHEN JUSTIFIED · USE DATA TO IMPROVE EDUCATION

PROPOSED / FOR ORGANISATIONAL REVIEW

Country: Uganda · Document Type: Education Data Governance, Analytics & Information-Sharing Framework · Version 1.0
August 2026 · www.scholanet.ug

01 Executive Summary

Scholanet Technologies is developing a national digital education ecosystem designed to connect learners, parents, teachers, schools, universities, colleges, TVET institutions, government, NGOs, donors, scholarship providers, employers and other education stakeholders.

A major component of the Scholanet ecosystem is the responsible collection, management, analysis and use of education-related information. Scholanet intends to use education data to help stakeholders understand:

- Learner locations
- School locations
- Enrolment patterns
- Learner movement
- Dropout risks
- Education access gaps
- Teacher distribution
- School capacity
- Scholarship needs
- Digital-learning participation
- Special-needs requirements
- Career & skills needs
- Education-sector trends

The purpose of this framework is to establish principles and controls for responsible education data governance. Scholanet recognises that education information may include personal data, including information concerning children.

Education data must be useful without compromising the privacy, dignity, safety or rights of the people represented by that data.

02 Purpose

This framework establishes how Scholanet should:

- Collect information
- Classify information
- Validate information
- Store information
- Analyse information
- Share information
- Protect information
- Retain information
- Delete information
- Respond to data incidents
- Provide responsible access to authorised stakeholders

03 Legal & Regulatory Foundation

Scholanet shall design its data governance programme with regard to applicable Ugandan laws and regulatory requirements, including the:

- Data Protection and Privacy Act, 2019
- Data Protection and Privacy Regulations, 2021
- Applicable electronic transactions & communications requirements
- Applicable child-protection & safeguarding requirements
- Other applicable laws & regulatory requirements

NITA-U identifies the Data Protection and Privacy Act, 2019 and the supporting Regulations, 2021 as the principal framework for protection of personal data in Uganda.

> This document is an organisational framework and does not replace professional legal advice or regulatory approval.

04 Core Principle

COLLECT RESPONSIBLY.
PROTECT CAREFULLY.
ANALYSE RESPONSIBLY.
SHARE ONLY WHEN JUSTIFIED.
USE DATA TO IMPROVE EDUCATION.

05 Data Governance Objectives

Scholanet aims to ensure that education data is:

- Accurate
- Relevant
- Secure
- Accessible to authorised users
- Protected from unauthorised use
- Used for legitimate purposes
- Appropriately retained
- Appropriately deleted or anonymised
- Responsibly shared

06 Data Categories

Scholanet may process different categories of information.

6.1 Learner Information

- Name, learner ID, school, class
- Education level, learning progress
- Enrolment & transfer information
- Attendance, scholarship status
- Learning activity, career interests

07 Parent & Guardian Information

- Name, contact information
- Relationship to learner
- Account information
- Authorised learner-management relationships

08 Teacher Information

- Name, professional information
- Teaching subjects, institution
- Qualifications, content profile
- Teaching activity
- Approved payment information where applicable

09 School Information

- Institution name, location, GPS
- Contact information, ownership category
- Education level, programmes, facilities
- Enrolment information
- Approved institutional contacts

> Only information necessary for a defined purpose should be collected.

10 Education Institution Database

Scholanet may maintain a national education institution directory containing information about:

Schools | Kindergartens | Colleges | Universities | TVET institutions | Vocational institutions | Special-needs institutions

Institutional information should be appropriately verified.

11 Location Data

Scholanet may use geographic information to support:

School discovery | School mapping | Education planning | Service coverage | Rural education analysis | Scholarship targeting

> Precise personal location information should not be publicly exposed unless there is an appropriate lawful and justified basis.

12 Dropout Data

Scholanet may develop systems for identifying learners who leave school, stop attending, become disengaged or experience barriers to continued education. The objective is not to label or stigmatise learners.

IDENTIFY SUPPORT RE-ENGAGE

13 Dropout Re-engagement

Where appropriate, Scholanet may help connect learners with:

Schools Online lessons Tutors Scholarships Education programmes Vocational pathways Community support

14 Girls' Education Data

Scholanet may support programmes addressing education interruptions affecting girls, including continued learning and re-entry pathways. Such information must be handled with heightened privacy and safeguarding considerations.

15 Special-Needs Data

Information relating to disability or special educational needs should receive appropriate protection, limited to authorised personnel who require it for legitimate educational or support purposes.

16 Child Data

Scholanet recognises that many users will be children. Child data requires additional safeguards, including age-appropriate privacy notices, parental/guardian controls, access controls, safeguarding procedures, limited public exposure, secure authentication and appropriate reporting mechanisms.

17 Data Minimisation

Scholanet shall seek to collect only information that is necessary, relevant, proportionate and connected to a defined purpose — avoiding collection simply because it might be useful in the future.

18 Purpose Limitation

Information collected for one purpose should not automatically be used for an unrelated purpose. Where a new purpose arises, Scholanet should assess whether the new processing is lawful and appropriate.

19 Data Accuracy

Scholanet shall seek to maintain accurate and up-to-date information. Users and authorised institutions should have appropriate mechanisms to correct inaccurate information, update information and report errors.

20 Data Validation

Institutional information may be verified through institution submissions, authorised administrators, approved records, verification processes and authorised government or institutional sources.

21 Data Ownership & Control

Data governance arrangements should clearly identify:

The data controller | Data processors | Authorised users | Data custodians | System administrators

The exact legal roles should be documented for each processing activity.

22 Data Processors

Third-party service providers that process personal data on behalf of Scholanet should be subject to appropriate contractual and security requirements. Examples may include:

Cloud providers | Hosting providers | Payment providers | Communication providers | Analytics providers | Technical service providers

23 Data Security

Scholanet should implement appropriate technical and organisational safeguards, including:

Encryption | Secure authentication | Role-based access | Access logging | Backups | Vulnerability management | Secure development | Monitoring | Incident response

The Data Protection and Privacy Act requires appropriate reasonable technical and organisational measures to protect personal data.

24 Role-Based Access

Users should only access information necessary for their role:

STUDENT	PARENT	TEACHER
Own authorised information	Authorised learner information	Authorised teaching information

SCHOOL	NGO	DONOR
Authorised institutional information	Authorised programme information	Approved aggregate impact information

GOVERNMENT
Authorised education-sector information

ScholaNeT

25 Government Data Access

Where formally authorised, Scholanet may provide government stakeholders with education-sector information to support:

Planning | Budgeting | Policy development | Resource allocation | Programme monitoring | Education access analysis

26 Government Reporting

Potential reports may include school distribution, enrolment trends, teacher distribution, education access, dropout trends, scholarship gaps and geographical education gaps.

Reports should use aggregated or appropriately protected information whenever individual identification is unnecessary.

27 NGO Data Access

Approved NGOs may receive information necessary for their authorised programmes — e.g. scholarship programmes, girls' education programmes, dropout re-engagement, disability programmes, rural education programmes.

28 Donor Data Access

Donors should generally receive impact information rather than unnecessary personal information — learners supported, schools supported, geographical coverage, programme progress, expenditure and outcomes.

29 Scholarship Data

Scholanet may maintain information required to identify scholarship opportunities, match eligible learners, track applications and monitor scholarship programmes. Sensitive information should be protected.

30 Data for Education Planning

Scholanet analytics may help identify underserved communities, areas with limited education access, teacher shortages, school capacity gaps, digital learning gaps and scholarship demand.

31 Education Analytics

Learner Analytics
- Enrolment
- Participation
- Retention
- Learning engagement

Teacher Analytics
- Teacher participation
- Subjects
- Content activity
- Tutoring activity

School Analytics
- Enrolment
- Institution capacity
- Services
- Geographical distribution

National Analytics
- Education access
- Dropout patterns
- Regional trends
- Education opportunities

32 Public Statistics

Scholanet may publish selected aggregate statistics where appropriate — number of institutions listed, registered learners, teachers, scholarship opportunities and education programmes.

> Public statistics must not unnecessarily expose identifiable personal information.

33 Data Anonymisation

Where individual identification is not required, Scholanet should consider anonymised or aggregated information.

34 Pseudonymisation

Where appropriate, personal identifiers may be separated from operational datasets through technical controls.

35 Research Data

Scholanet may collaborate with researchers and universities. Research access should be:

Purpose-specific | Authorised | Documented | Privacy-conscious

36 Data Sharing Agreements

Where significant information is shared with another organisation, an appropriate agreement may define:

Purpose | Information shared | Permitted use | Security | Retention | Deletion | Confidentiality | Incident reporting | Responsibilities

37 International Data Transfers

Where personal information is processed or stored outside Uganda, Scholanet should assess applicable legal requirements and safeguards before the transfer.

The Data Protection and Privacy Act specifically addresses processing or storage of personal data outside Uganda.

38 Third-Party Services

Before integrating third-party systems, Scholanet should evaluate:

Security | Privacy | Reliability | Contractual protections | Data location | Access controls | Breach procedures

39 Payment Data

Payment providers should process payment information according to applicable requirements. Scholanet should avoid storing sensitive payment credentials unnecessarily, using appropriately authorised payment providers where possible.

40 Donation Data

Scholanet may maintain records such as donor reference, contribution, programme, date and transaction status. Public donor recognition should respect donor preferences and applicable privacy requirements.

41 Data Retention

Scholanet should establish retention periods based on:

- Legal requirements
- Operational needs
- Contractual requirements
- Safeguarding
- Legitimate programme requirements

Personal data should not be retained indefinitely without justification.

42 Data Deletion

When information is no longer required and there is no lawful reason to retain it, Scholanet should securely delete, destroy or appropriately de-identify it.

43 Backups

Backups should be secure, access-controlled, monitored, tested and subject to appropriate retention rules.

44 Data Breach Management

Scholanet should maintain a formal incident-response process. Potential incidents include:

- Unauthorised access
- Lost information
- Stolen credentials
- Malware
- Accidental disclosure
- System compromise

45 Incident Response



46 Privacy Impact Assessments

Before introducing high-risk processing activities, Scholanet should assess what information is collected, why it is collected, who can access it, potential risks and mitigation measures.

NITA-U's regulatory guidance identifies Privacy Impact Assessments and privacy-by-design as important components of data-protection governance.

47 Privacy by Design

Privacy should be considered during:

- Product design
- Database design
- Application development
- Feature development
- Analytics
- Integrations
- Deployment

48 Privacy by Default

Default settings should favour privacy, for example:

- Minimum necessary profile visibility
- Restricted child information
- Limited third-party access
- Secure account defaults

ScholaNeT

49 User Rights

Scholanet should establish mechanisms for users to exercise applicable rights relating to their personal information, including access, correction, deletion where applicable, restriction, objection and portability where applicable.

NITA-U's published privacy notice describes these rights under Uganda's data-protection framework.

50 Data Subject Requests

1. Receiving a request
2. Verifying identity where necessary
3. Assessing the request
4. Responding within applicable requirements
5. Recording the outcome

51 Child Data Requests

Requests concerning children's information should be handled with appropriate safeguarding and authority checks.

52 Parental Access

Parents or guardians may receive access to learner information only where the relationship and authority are appropriately established.

53 Account Security

Users should be encouraged and, where appropriate, required to use strong passwords, multi-factor authentication, secure recovery mechanisms and verified contact information.

54 Administrator Security

Administrative accounts should have enhanced controls: multi-factor authentication, privileged access management, audit logs, restricted access and periodic review.

55 Audit Logging

Important actions should be logged where appropriate:

- Login
- Account changes
- Permission changes
- Data exports
- Administrative access
- Data deletion

56 Data Exports

Bulk data exports should require appropriate authorisation. Every sensitive export should have an authorised purpose, responsible user, date, destination and appropriate security.

57 Public API

If Scholanet eventually provides APIs, access should be controlled through authentication, authorisation, rate limiting, monitoring, secure keys and data minimisation.

58 Data Quality

Scholanet should monitor:

Duplicates | Incomplete records | Inconsistent information | Outdated records | Invalid institutional information

59 Data Quality Dashboard

Administrators may monitor:

Completeness | Accuracy | Duplication | Verification status | Update frequency

60 National School Directory

The school directory should distinguish between:

Verified institution | Pending verification | Inactive institution | Duplicate institution | Institution requiring review

ScholaNeT

61 GPS & School Mapping

School location information may support navigation, school discovery, planning and geographic analysis.

> Exact residential locations of children should not be publicly exposed merely for mapping purposes.

62 Education Gap Maps

Scholanet may produce maps showing aggregate gaps such as school shortages, teacher shortages, digital-access gaps and scholarship demand.

63 Donor Targeting

Where lawful and appropriate, aggregate data may help donors identify regions requiring support, education programmes requiring funding, underserved populations and infrastructure needs.

64 Scholarship Matching

Scholanet may use authorised information to match learners with suitable scholarship opportunities. Matching logic should be transparent enough to identify and correct material errors.

65 Dropout Alerts

Where the platform uses indicators to identify possible dropout risk, such indicators should be treated as signals requiring appropriate human review rather than automatic conclusions.

66 AI & Automated Decision-Making

If Scholanet uses artificial intelligence or automated systems, the organisation should assess:

Accuracy | Bias | Explainability | Security | Privacy | Human oversight

> AI should not automatically make high-impact decisions about learners without appropriate safeguards.

67 Responsible Education Analytics

Analytics should be used to:

Identify problems | Improve services | Support planning | Allocate resources responsibly

Analytics should not be used to unfairly label or stigmatise learners.

ScholaNeT

68 Education Dashboards

Potential dashboards, each exposing only authorised information:

69 Government Dashboard
Institution distribution, enrolment trends, dropout trends, teacher distribution, education access, scholarship gaps.

70 NGO Dashboard
Programme beneficiaries, geographical coverage, programme progress, intervention outcomes.

71 Donor Dashboard
Funds contributed, programme supported, aggregate beneficiaries, progress, outcomes.

72 School Dashboard
Learners, teachers, attendance, learning activities, parent communication, institutional operations.

73 Teacher Dashboard
Classes, lessons, content, tutoring, learner engagement, earnings where applicable.

74 Parent Dashboard
Attendance, learning, school, communication, opportunities for authorised learners.

75 Learner Dashboard
Age-appropriate lessons, learning materials, school information, scholarships, career guidance, authorised progress information.

Scholanet Administration Dashboard
Full authorised technical and operational oversight.

76 Data Governance Committee

Scholanet may establish a Data Governance Committee responsible for:

Data policy | Privacy | Security | Data quality | Access governance | Risk review

77 Data Protection Officer

Where required or appropriate, Scholanet should appoint a responsible Data Protection Officer or equivalent privacy lead, responsible for privacy compliance, data-protection advice, incident coordination, data-subject requests, staff awareness and policy review.

78 Staff Training

Relevant employees and contractors should receive training on privacy, cybersecurity, confidentiality, safeguarding and responsible data use.

79 Partner Training

Partners receiving sensitive information may be required to demonstrate appropriate data-protection practices.

80 Confidentiality

Employees, contractors and partners should protect confidential information accessed through Scholanet.

81 Data Classification

Scholanet may classify information as:

PUBLIC
Information intentionally made public.

INTERNAL
Information intended for authorised Scholanet personnel.

CONFIDENTIAL
Information requiring restricted access.

HIGHLY RESTRICTED
Highly sensitive information requiring enhanced controls.

82 Example Data Classification

Information	Classification
Public school name	Public
School public contact	Public
Teacher public profile	Controlled/Public where authorised
Parent contact	Confidential
Learner academic record	Highly Restricted
Learner safeguarding information	Highly Restricted
Donor programme report	Confidential/Public where approved
Aggregate national statistics	Public where approved

ScholaNeT

83 Data Access Review

Access privileges should be periodically reviewed. Users who no longer require access should have permissions removed.

84 Employee Exit

When employees or contractors leave Scholanet: accounts should be disabled, access should be revoked, credentials should be reviewed, and organisational equipment should be recovered where applicable.

85 Vendor Exit

When a third-party service relationship ends, Scholanet should address data return, data deletion, access revocation, credential rotation and contractual obligations.

86 Data Sharing Principle

Before sharing information, Scholanet should ask:

1. Why is it needed?
2. Who needs it?
3. What information is necessary?
4. Is there an appropriate legal basis?
5. What safeguards exist?
6. How long will it be retained?

87 Prohibited Data Practices

Scholanet should not knowingly:

- Sell learner personal data without lawful authority
- Expose private learner information publicly
- Provide unrestricted access to sensitive databases
- Use children's information for unrelated purposes
- Share information merely because it is technically possible

88 Data for Fundraising

Fundraising campaigns may use aggregate education needs, for example: "A programme requires support for 5,000 learners in underserved communities."

Individual learner information should not be published unnecessarily.

89 Donor Transparency Without Privacy Violation

Scholanet should demonstrate impact without exposing vulnerable learners. The preferred approach is:

DONOR → PROGRAMME → AGGREGATE IMPACT → OUTCOME

rather than exposing unnecessary individual information.

90 Data for Education Policy

Scholanet may support authorised stakeholders with aggregate information useful for education planning, budgeting, resource allocation, infrastructure planning, teacher planning and digital education planning.

91 Data for NGOs

NGOs may use approved data to identify programme areas, education gaps, scholarship demand and vulnerable populations.

92 Data for Research

Research collaborations should establish research purpose, dataset, access restrictions, security, publication requirements and privacy safeguards.

93 Data for Innovation

Where appropriate, anonymised datasets may support innovation in education technology, research, analytics, artificial intelligence and education planning.

94 Data Ethics

Scholanet shall seek to ensure that data-driven innovation does not undermine:

Dignity | Equality | Privacy | Safety | Educational opportunity

95 Accountability

Every major data-processing activity should have a responsible owner.

96 Data Governance Register

Scholanet should maintain a register containing, where appropriate:

- Processing activity
- Purpose
- Data category
- Users
- Legal basis
- Retention
- Processors
- Safeguards

97 Data Flow Mapping

Scholanet should document major data flows:

LEARNER → SCHOLANET → SCHOOL SERVICES → AUTHORISED ANALYTICS → APPROVED STAKEHOLDERS

Data flows involving third parties should be documented.

98 Data Protection Impact Review

New high-risk features should undergo privacy and security review before production deployment, for example:

- Biometric identification
- Location tracking
- Automated learner profiling
- Large-scale data matching
- Sensitive health/disability information
- New external integrations

99 Security Testing

Scholanet should periodically conduct appropriate:

Vulnerability assessments | Penetration testing | Access reviews | Backup testing | Incident simulations

100 Continuous Improvement

Data governance should evolve as Scholanet grows. The controls required for 10,000 users may not be sufficient for 1,500,000 learners and 48,000 institutions. Scholanet should therefore continuously strengthen:

Infrastructure | Cybersecurity | Privacy | Governance | Staffing | Monitoring

101 National-Scale Data Principle

At national scale, Scholanet must treat education information as a strategic responsibility.

The objective is not simply to possess a large database. The objective is to build a trusted education information ecosystem.

102 Data Governance Maturity

Scholanet may progressively develop through:

Stage 1 — Foundation

- Basic privacy controls
- Secure accounts
- Data policies

Stage 2 — Controlled Growth

- Role-based access
- Audit logs
- Formal data-sharing agreements

Stage 3 — Institutional Scale

- Advanced analytics
- Governance committee
- Formal privacy programme
- Regular audits

Stage 4 — National Scale

- Advanced security
- High-availability infrastructure
- Sophisticated data governance
- National-level reporting
- Mature incident response

103 Key Performance Indicators

Data accuracy | Data completeness | Privacy incidents | Security incidents | Data-subject requests | Request-resolution times | Unauthorised access attempts | Verified institutions | Duplicate records | Outdated records

104 Annual Data Governance Report

Scholanet may publish an annual high-level report containing data governance improvements, security improvements, privacy initiatives, aggregate impact, major incidents where appropriate, and future priorities.

105 – 109 Stakeholder Requirements

105 Partner Requirements

- Protect the information
- Use it only for approved purposes
- Prevent unauthorised disclosure
- Report incidents
- Delete or return information where required

106 School Requirements

- Provide accurate information
- Protect account credentials
- Restrict access
- Respect learner privacy
- Report suspected incidents

107 Teacher Requirements

- Protect learner information
- Avoid unauthorised disclosure
- Use information only for legitimate educational purposes
- Report suspected abuse or security incidents through appropriate channels

108 Parent Responsibilities

- Protect account credentials
- Use learner information responsibly
- Avoid publicly sharing sensitive information about children
- Report suspicious activity

109 Learner Safety — Learners should be protected from unnecessary exposure, harassment, exploitation, inappropriate data sharing and unauthorised contact.

110 Public Portal Data

The public portal should contain only information intentionally designated for public access — public institution information, approved partner information, public programmes, scholarship opportunities, educational resources and public impact statistics.

111 Private Portal Data

Private information should remain behind authenticated access controls.

112 Data Governance & Trust

Scholanet's long-term value depends on public trust, demonstrated through:

Transparent policies | Secure systems | Responsible data practices | Accountable partnerships | Appropriate user controls

113 Implementation Priorities

Before national-scale deployment, Scholanet should prioritise:

1. Data inventory
2. Data classification
3. Privacy assessment
4. Access-control architecture
5. Security architecture
6. Data retention schedule
7. Incident-response plan
8. Data-sharing agreements
9. Privacy notices
10. Staff training
11. Vendor due diligence
12. Regular security testing

114 Future Data Platform

Scholanet may eventually develop an integrated:

SCHOLANET EDUCATION INTELLIGENCE PLATFORM

capable of supporting:

National school mapping | Education dashboards | Learner analytics | Teacher analytics | Scholarship matching | Dropout intervention | Education planning | Donor reporting | NGO programme management

115 Responsible National Impact

Scholanet's objective is not to replace government education systems. Where appropriate, Scholanet should seek to complement existing systems and support authorised stakeholders through responsible digital services and information.

116 Governance Principle

The larger Scholanet becomes, the stronger its governance must become. Growth should never be used as a justification for weakening:

Privacy | Security | Safeguarding | Accountability

117 Final Commitment

Scholanet Technologies is committed to building an education ecosystem in which information is used responsibly to expand opportunity. The organisation's guiding principle is:

DATA SHOULD HELP PEOPLE, NOT HARM PEOPLE.

118 Document Status

Document	Education Data Governance, Analytics & Information-Sharing Framework
Version	1.0
Status	Proposed / For Organisational Review
Owner	Scholanet Technologies
Review Cycle	At least annually or whenever significant legal, organisational, technological or platform changes occur.

Note: This is a proposed data governance and analytics framework for organisational review. Unless expressly identified as operational or verified, statements regarding systems, controls, dashboards and compliance represent planning intentions rather than confirmed or audited implementations. Formal legal advice should be obtained before production launch.

CONNECTING EDUCATION. CONNECTING OPPORTUNITY. CONNECTING THE FUTURE.