



SCHOLANET TECHNOLOGIES

DATA GOVERNANCE, PRIVACY, DATA PROTECTION & CHILD SAFEGUARDING FRAMEWORK

PROTECTING **LEARNERS**, PARENTS, TEACHERS, INSTITUTIONS, PARTNERS & EDUCATION DATA



"Protect Data. Protect People. Enable Trust."



Schola

01 Purpose of This Framework

This framework establishes the principles, controls and responsibilities that Scholanet Technologies intends to use to protect personal data processed through the Scholanet ecosystem.

Scholanet is designed to connect learners, parents and guardians, teachers, schools, universities, colleges, TVET and VTI institutions, special-needs education providers, scholarship providers, NGOs, donors, government stakeholders, businesses, youth entrepreneurs and education partners.

Because the platform may process information relating to children, families, education, institutions and other individuals, privacy and responsible data governance are fundamental requirements of the system.

02 Legal & Regulatory Basis

Scholanet intends to design and operate its data-processing activities in accordance with applicable Ugandan law and regulatory requirements. The principal framework includes:

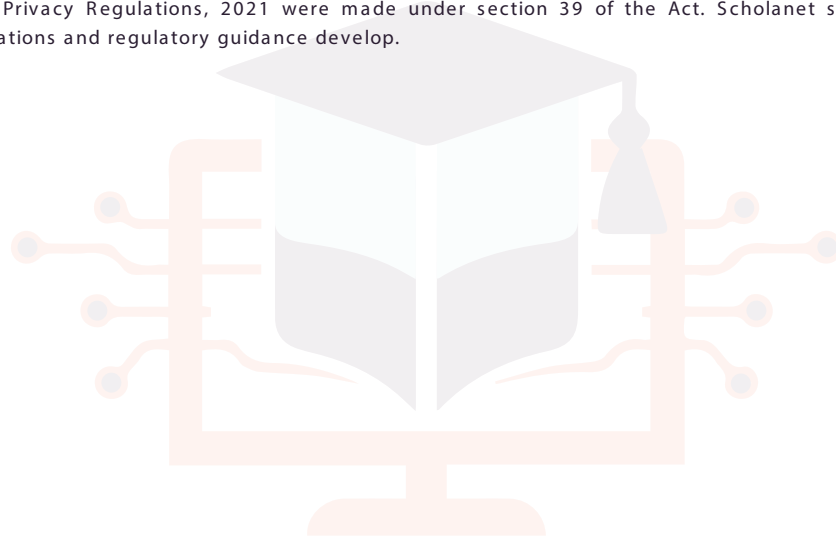
Data Protection and Privacy Act, 2019 (Act No. 9 of 2019)

Data Protection and Privacy Regulations, 2021

NITA-U & Personal Data Protection Office guidance

Applicable cybersecurity, e-transactions, children & education laws

The Data Protection and Privacy Regulations, 2021 were made under section 39 of the Act. Scholanet shall review this framework periodically as laws, regulations and regulatory guidance develop.



ScholaNet

03 Important Legal Disclaimer

This document is an organisational framework and is not a substitute for formal legal advice.

Before production launch and especially before processing large volumes of personal data, Scholanet should obtain professional legal and data-protection advice and complete all applicable registration, compliance, contractual and governance requirements.

The organisation should also assess whether it is required to register as a data collector, data processor and/or data controller under the applicable Ugandan framework.

04 Data Protection Vision

Scholanet's data protection vision is:

"PROTECT DATA. PROTECT PEOPLE. ENABLE TRUST."

Technology should make education more accessible without unnecessarily exposing the people who use the system.



ScholaNet

05 Core Data Protection Principles

Scholanet shall seek to apply the following principles:

- 1 Lawfulness
- 2 Fairness
- 3 Transparency
- 4 Purpose limitation
- 5 Data minimisation
- 6 Accuracy
- 7 Storage limitation
- 8 Security
- 9 Accountability
- 10 Privacy by design
- 11 Privacy by default
- 12 Responsible data sharing

The Act regulates the collection and processing of personal information and establishes obligations for data collectors, data processors and data controllers.

ScholaNet

06 What Is Personal Data?

For Scholanet purposes, personal data may include information that identifies or can reasonably identify an individual. Examples may include:



The Ugandan Data Protection and Privacy Act defines personal data broadly, including information relating to identity, educational level, occupation and identifying numbers or particulars.

07 Scholanet Data Categories

Scholanet may process different categories of data depending on the service:



ScholaNet

7.1 – 7.7 Data Categories

7.1 Account Data

- Name
- Phone number
- Email
- Username
- Account credentials

7.2 Education Data

- Learner identification
- Institution & class
- Academic information
- Attendance & participation
- Education history

7.3 Parent Data

- Parent identity
- Contact information
- Relationship to learner
- Linked learner accounts

7.4 Teacher Data

- Professional information
- Qualifications
- Teaching subjects
- Institution & content profile
- Platform activity

7.5 Institution Data

- Institution identity
- Location
- Contact information
- Registration information
- Available services

7.6 Scholarship Data

- Applications
- Eligibility information
- Supporting documentation
- Application status

7.7 Payment Data

- Transaction reference
- Payment status
- Donor information where necessary
- Contribution amount

Payment-card and sensitive financial information should, where possible, be handled by appropriately authorised payment providers rather than stored unnecessarily by Scholanet.



Scholanet

08 Data Minimisation

Scholanet should collect only information reasonably necessary for a defined purpose. The system should ask:

"Do we actually need this information?"

If the answer is no, the information should not be collected merely because it could be useful in the future.

09 Purpose Limitation

Information collected for one purpose should not automatically be reused for unrelated purposes. For example, information collected to register a learner should not automatically be used for:

Advertising Commercial profiling Unrelated marketing Selling personal information

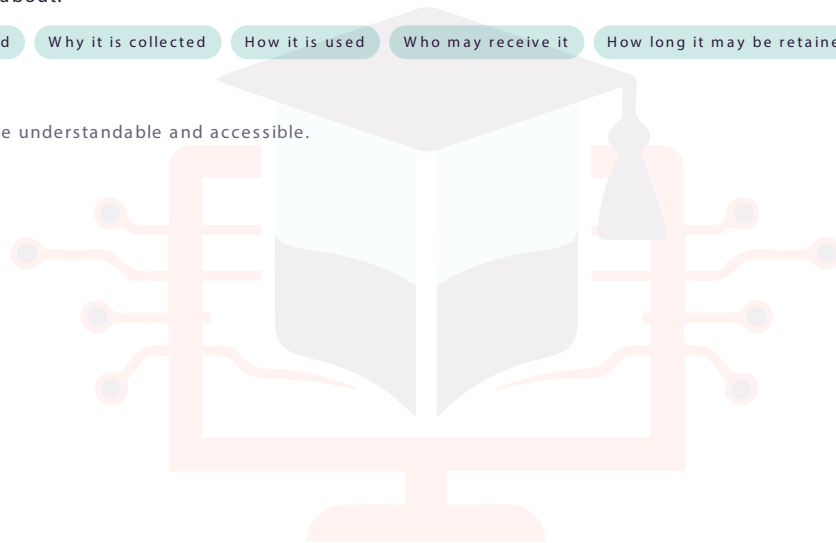
Any additional use must have an appropriate lawful basis and comply with applicable requirements.

10 Transparency

Users should be informed about:

What information is collected Why it is collected How it is used Who may receive it How long it may be retained How to exercise rights
How to raise a complaint

Privacy information should be understandable and accessible.



ScholaNet

11 Lawful Processing

Scholanet shall establish and document an appropriate lawful basis for processing personal data. Depending on the activity, this may include:

Consent Performance of a contract Legal obligation Legitimate interests where applicable Other lawful grounds under Ugandan law

Consent should not be treated as a universal solution. The correct legal basis should be assessed for each processing activity.

12 Consent

Where consent is relied upon, Scholanet should ensure that consent is:

Informed

The person understands what they are consenting to.

Specific

Consent relates to a clearly defined purpose.

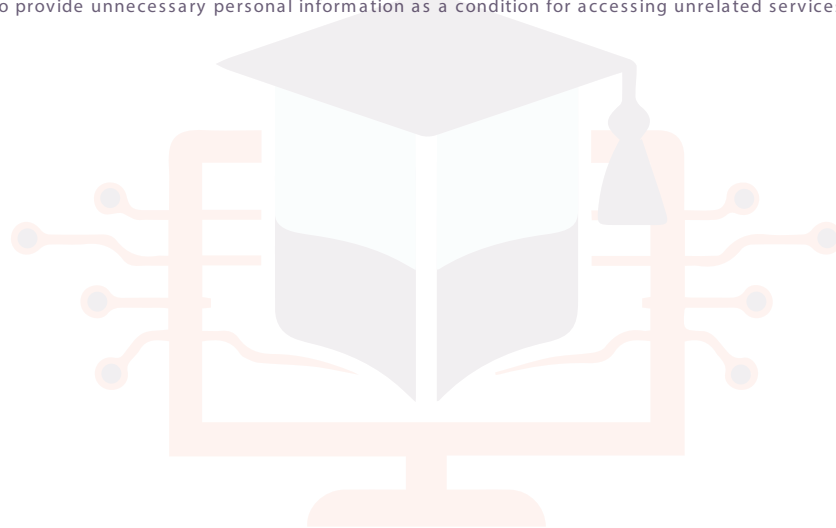
Appropriately Recorded

Evidence of consent is retained and traceable.

Freely Given & Withdrawable

Given without undue pressure and capable of withdrawal where applicable.

Users should not be forced to provide unnecessary personal information as a condition for accessing unrelated services.



ScholaNet

13 Child Data

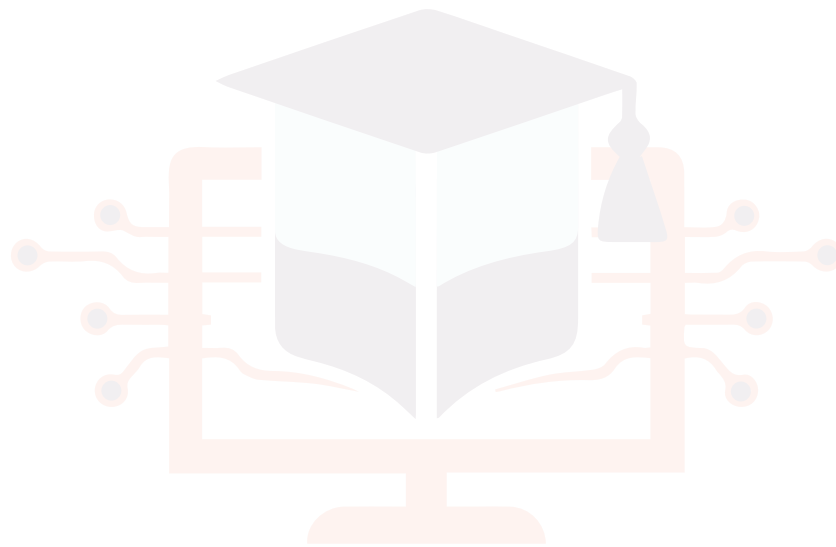
Scholanet is expected to serve children and therefore requires enhanced protection for children's information. Children's data should be processed only for legitimate, clearly defined purposes and with appropriate safeguards.

Where parental or guardian involvement is required by applicable law or the nature of the service, Scholanet should implement appropriate mechanisms for verification and consent.

14 Child Safeguarding

Scholanet shall treat child safeguarding as a core platform requirement. The system should protect children from:

- Exploitation
- Abuse
- Inappropriate contact
- Exposure of private information
- Harmful content
- Unauthorised profiling
- Inappropriate commercial activity



ScholaNet

15 Children's Public Profiles

Scholanet should not publicly expose unnecessary personal information about children. Public-facing pages should avoid displaying information such as:

Private phone numbers

Private addresses

Exact personal locations

Confidential education records

Sensitive family information

Scholarship application details

16 Child Photographs & Videos

Images and videos involving children should only be collected, published or shared under appropriate policies and lawful permissions. Public campaigns should avoid unnecessary identification of children.

Where appropriate, Scholanet may use:

Anonymised stories

First names only

Non-identifying photographs

Aggregated statistics



17 Sensitive Information

Some information may create increased risk if improperly disclosed. Examples may include:

Disability information Health-related information Pregnancy-related information Family circumstances Safeguarding cases
Financial hardship Scholarship vulnerability Disciplinary information

Such information should receive enhanced access controls.

18 Education Dropout Data

Scholanet intends to help identify and support learners who may have interrupted their education. This data must be handled carefully. A learner should not be publicly labelled as "dropout", "failed", "problem learner" or another potentially harmful label.

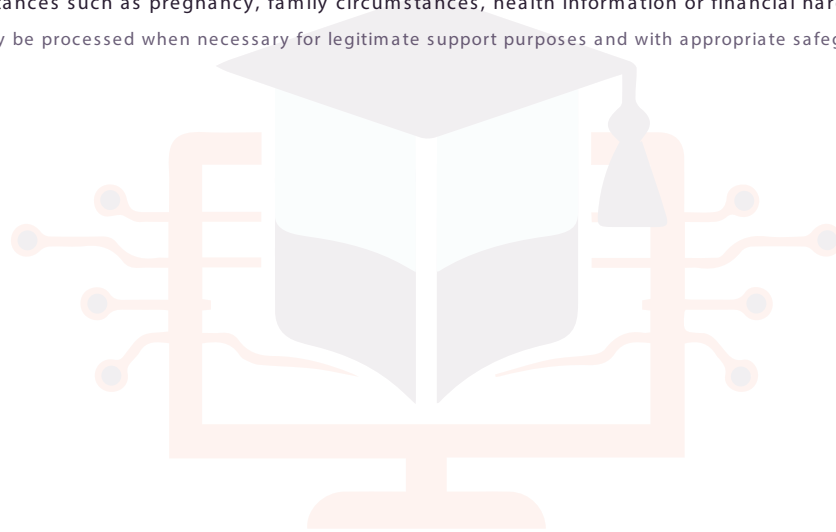
Internal systems should use respectful terminology such as:

Education interruption Re-engagement case Support required Referral required

19 Girls' Education Data

Information relating to girls who experience education interruption requires heightened sensitivity. Scholanet should not publicly disclose personal circumstances such as pregnancy, family circumstances, health information or financial hardship.

Such information should only be processed when necessary for legitimate support purposes and with appropriate safeguards.



ScholaNet

20 Scholarship Data

Scholarship information should be accessible only to authorised users. Scholarship providers should receive only the information necessary for:

Eligibility assessment Application processing Programme administration Reporting

21 Location Data

Scholanet may use school geographic information and, where appropriately authorised, user location information. Location data should be necessary, purpose-specific and appropriately protected. Exact personal location should not be publicly exposed unnecessarily.

22 School Location Data

Public information about registered education institutions may include institution name, general location, contact details, GPS location and services offered — distinguished from the private location of an individual learner or parent.



Scholanet

23 Data Accuracy

Scholanet should take reasonable steps to ensure that personal information is accurate, complete where necessary and current where required. Users should have mechanisms to request correction of inaccurate information.

24 User Access Rights

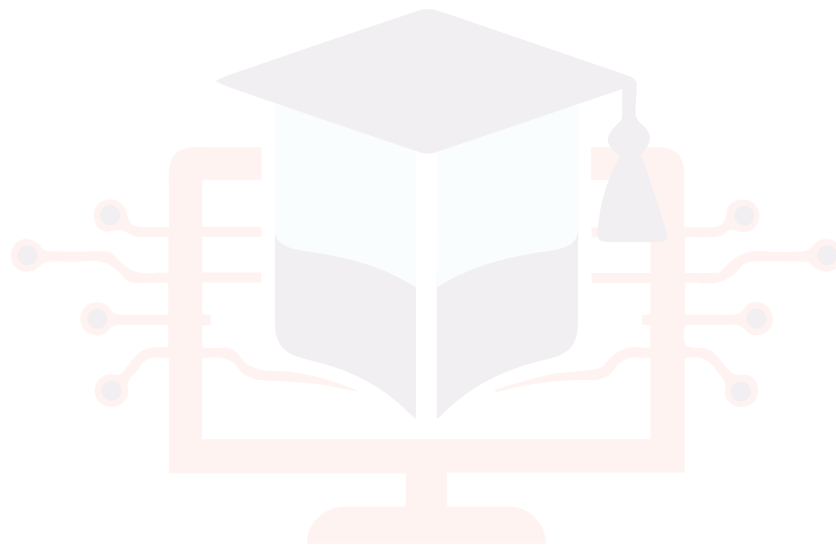
Subject to applicable law and appropriate verification, users should be able to request information about personal data held about them. Scholanet should establish procedures for:

Identity verification Request submission Response Correction Restriction where applicable Deletion where legally applicable

25 Right to Rectification

Where personal information is inaccurate or incomplete, users should have an appropriate mechanism to request correction. Examples include:

Incorrect name Incorrect contact Incorrect school Incorrect qualification Incorrect profile information



ScholaNet

26 Right to Erasure

Where legally applicable, users may request deletion of personal information. However, deletion may not always be immediately possible where Scholanet has a lawful obligation or legitimate reason to retain certain information.

The system should distinguish between:

Account deletion

Data deletion

Anonymisation

Retention required by law

Records for legitimate operational purposes

27 Data Portability

Where applicable, Scholanet should provide users with appropriate access to their information in a structured and commonly usable format.

28 Right to Object or Restrict

Where applicable, users may have rights to object to or restrict certain forms of processing. Scholanet should establish a process for receiving and assessing such requests.



ScholaNet

29 Privacy by Design

Privacy must be incorporated during system development rather than added after the platform is completed. Every new module should undergo a privacy review, for example:

Learner registration Parent portal Teacher Studio School management Scholarships Marketplace Donations Analytics
Government reporting

30 Privacy by Default

The default system configuration should provide the highest reasonable level of privacy. Examples:

Private Profiles

Private profiles by default for all users.

Minimum Visibility

Minimum data visibility unless explicitly needed.

Restricted Child Information

Enhanced restrictions on children's information.

Role-Based Access & Limited Sharing

Access tied to role, with sharing kept to a minimum.

Users should not have to understand complicated privacy settings just to remain reasonably protected.



ScholaNet

31 Role-Based Access

Different users should see different information:

LEARNER	PARENT
Own authorised information	Authorised linked learner information
TEACHER	SCHOOL
Authorised teaching information	Authorised institutional information
NGO	DONOR
Authorised programme information	Aggregated / authorised impact information
GOVERNMENT PARTNER	SYSTEM ADMINISTRATOR
Authorised aggregated or agreed data	Controlled technical access

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