

eduID.ng

Federation Policy

Version 2.0

Document owner	Assembly of Members (AoM)
Drafting body	Policy Review Working Group (PRWG), under delegation from the AoM
Federation Operator	Eko-Konnect Research and Education Initiative
Approval status	Ratified by the Assembly of Members, 25 September 2026
Effective date	28 September 2026
Supersedes	eduID.ng Policy Document dated 25 November 2021
Version	2.0

PART I - CORE FEDERATION POLICY

1. Definitions

Term	Meaning
Assembly of Members or AoM	the body comprising Federation Members and holding the ultimate member and constitutional authority of eduID.ng.
Attribute	information describing an End User, including an identifier, affiliation, entitlement, role or assurance information.
Council	the eduID.ng Federation Council established under this Policy to exercise continuing oversight under authority delegated by the AoM.
Digital Identity	a set of identifiers and Attributes associated with an End User and managed through an identity-management lifecycle.
End User	a natural person whose Digital Identity is used to access a Participating Service.
Entity	an Identity Provider, Service Provider, Attribute Authority, discovery service, proxy or other technical component registered by the Federation.
Federation	the Nigerian research and education identity federation known as eduID.ng.
Federation Member or Member	an eligible organisation admitted to eduID.ng and bound by this Policy.
Federation Operator or Operator	the organisation designated to provide the technical and administrative operation of eduID.ng.
Home Organisation	a Member responsible for managing and asserting Digital Identities for its End Users.
Interfederation	an arrangement enabling trust and access between eduID.ng and another federation or aggregation service, including eduGAIN.

Participating Service	a service registered, enabled or integrated under edulD.ng, whether operated by a Member, the Operator or another approved provider.
Policy Instrument	the Core Policy, a Schedule, Profile, Procedure, standard, form or decision made under this Policy.
Profile	a controlled technical, security, assurance, attribute or service specification adopted under this Policy.
Service Provider	an organisation or Entity offering a service that relies on federated authentication, Attributes or another approved trust mechanism.
Working Group	a time-limited or standing group established by the AoM or Council under Schedule A.

2. Status, purpose and principles

2.1 Status. edulD.ng is Nigeria's national identity federation for the research and education community and continues the federation governed by the policy dated 25 November 2021.

2.2 Purpose. The Federation enables trusted access to research, education and community services through common governance, technical, security, privacy and assurance arrangements, and supports approved Interfederation participation including eduGAIN.

2.3 Principles. The Federation shall be community governed, transparent, inclusive, proportionate, secure, privacy-respecting, interoperable, sustainable and responsive to the needs of Nigerian research and education.

2.4 Continuity. Adoption of this Policy does not create a new federation and does not require existing Members to reapply, although the Operator may require records, contacts, agreements or compliance evidence to be refreshed.

3. Policy framework and authority

3.1 Policy hierarchy. The Core Policy prevails over all other Policy Instruments. Schedules form part of this Policy. Profiles and Procedures must be consistent with the Core Policy and Schedules.

3.2 Authority. The AoM approves and amends the Core Policy and reserved constitutional provisions. It may delegate approval of Schedules, Profiles and Procedures as specified in this Policy.

3.3 Public register. The Operator shall maintain a public register of current Policy Instruments showing version, approval authority, approval date, effective date and superseded version.

3.4 Compliance. Members and participating organisations shall comply with the Policy Instruments applicable to the roles, Entities and services they operate or adopt.

4. Community governance

4.1 Assembly of Members. The AoM is the ultimate member and constitutional authority of edulD.ng. It approves the Core Policy and reserved matters, elects or confirms community representatives, delegates defined responsibilities and holds the Council and Operator accountable.

4.2 Federation Council. The Council provides strategic, policy, risk and sustainability oversight between AoM meetings. It may exercise only the powers conferred by this Policy or delegated by the AoM and shall report to the AoM.

4.3 Working groups. The AoM or Council may establish standing or time-limited Working Groups with written terms of reference. A Working Group makes recommendations and has no independent decision-making authority unless expressly delegated.

4.4 Technical Committee. The Technical Committee advises on architecture, Profiles, interoperability, assurance, security and service integration. Its composition and operation are governed by Schedule A.

4.5 Governance rules. Composition, election, meetings, voting, conflicts of interest, reporting and reserved matters are set out in Schedule A.

5. Federation Operator

5.1 Designation. Eko-Konnnect Research and Education Initiative is designated as Federation Operator, subject to this Policy and an operating framework approved through the Federation's community governance processes.

5.2 Core responsibilities. The Operator shall securely administer the Federation; manage registration and metadata services; support Members; implement authorised decisions; maintain documentation and registers; coordinate incidents; support Interfederation; and provide secretariat support as assigned.

5.3 Accountability. The Operator shall provide an annual operational, security, service, risk and financial report to the Council and AoM and shall disclose material incidents, conflicts and service dependencies.

5.4 Operational independence. The Operator may take routine technical and administrative decisions within approved Policy Instruments. It shall not determine constitutional or community policy matters except where expressly delegated.

5.5 Emergency action. The Operator may take proportionate temporary action necessary to protect security, trust or continuity, subject to prompt notice, recorded reasons and review under clause 15.

6. Membership and participation

6.1 Eligibility. Membership is open to accredited or legally recognised Nigerian higher-education institutions, research organisations and other organisations whose primary purpose supports research and education. Service providers and other public-interest organisations may participate under the class and conditions specified in Schedule B.

6.2 Admission. Applications shall be assessed transparently against published legal, organisational, technical, security and contact requirements. Routine compliant applications may be approved by the Operator under delegated authority; exceptions and refusals shall be decided or reviewed by the Council.

6.3 No automatic entitlement. Eligibility does not create an automatic right of admission or access to every Profile, service or Interfederation arrangement.

6.4 Member register. The Operator shall publish a register of Members, registered Entities, adopted Profiles and Participating Services, subject to security and data-protection restrictions.

7. General obligations of Members

7.1 Contacts. Maintain current executive or administrative, technical, security and privacy contacts and validate them at least annually.

7.2 Secure operation. Operate registered systems and Entities securely, apply relevant Profiles, manage vulnerabilities and cooperate in testing and incident response.

7.3 Accuracy. Ensure registration, metadata, identity and Attribute information is accurate, authoritative, current and promptly corrected or withdrawn when no longer valid.

7.4 Law and policy. Comply with applicable Nigerian law, this Policy and all adopted Policy Instruments.

7.5 User support. Provide first-line support to its End Users and escalate only relevant federation issues through authorised contacts.

7.6 Notification. Notify the Operator promptly of material organisational, technical, security, privacy, ownership or contact changes affecting participation.

7.7 Acceptable use. Ensure End Users are subject to appropriate acceptable-use and privacy information.

7.8 Costs. Pay approved charges and bear its own implementation and operational costs unless otherwise agreed.

8. Identity Providers, Attributes and assurance

8.1 Identity lifecycle. A Home Organisation shall maintain documented processes for identity proofing, enrolment, credential issuance, authentication, changes, suspension and timely deprovisioning.

8.2 Practice statement. A Home Organisation shall provide an Identity Management Practice Statement in the form required by the applicable assurance Profile.

8.3 Authentication. Credentials and authentication controls shall be proportionate to risk and comply with applicable Profiles, including multi-factor authentication where required.

8.4 Attributes. Attributes shall be sourced authoritatively, kept accurate and released only where necessary and permitted. Persistent identifiers shall be scoped and managed to reduce correlation and misuse.

8.5 Assurance. A Member shall claim only assurance levels and entity categories for which it has been assessed or self-declared in accordance with the relevant Profile.

9. Service Providers and integrated services

9.1 Access decisions. A Service Provider remains responsible for determining who may access its service, the access rights granted and the Attributes it requires.

9.2 Data minimisation. A Service Provider shall request and process only Attributes reasonably necessary for the stated service purpose and shall publish appropriate privacy and support information.

9.3 Service integration. The Federation may enable or integrate services that advance research and education. Each service shall have an approved service schedule defining ownership, eligibility, trust, privacy, security, support, sustainability, suspension and exit arrangements.

9.4 Service register. The Operator shall maintain a public register of approved Participating Services and their applicable schedules and contacts.

9.5 Relationship with geteduroam and eduroam. eduID.ng may provide federated identity, institutional eligibility verification and related capabilities to support geteduroam onboarding. Such use does not make eduroam part of the eduID.ng identity federation. Membership of eduID.ng does not automatically confer participation in eduroam, and successful eduID.ng authentication does not itself grant network access. eduroam authentication, RADIUS or RadSec infrastructure, realm routing, roaming, network access, logging, security and compliance remain governed by the applicable national and global eduroam policies.

10. Data protection and privacy

10.1 Applicable law. Each participant shall comply with the Nigeria Data Protection Act 2023 and applicable regulations, directives and guidance, as amended or replaced.

10.2 Responsibility. Each participant is responsible for determining and documenting its role and lawful basis for personal-data processing. Federation participation does not by itself make all participants joint controllers.

10.3 Principles. Personal data shall be processed lawfully, fairly and transparently; limited to specified purposes; minimised; accurate; retained no longer than necessary; and protected by appropriate safeguards.

10.4 Transparency. Members and Service Providers shall provide clear privacy information covering federated authentication, Attribute release, logs, recipients, retention, rights and relevant cross-border processing.

10.5 Cooperation. Participants shall cooperate on data-subject requests, complaints, breaches, impact assessments and regulatory enquiries where their processing is involved.

10.6 Metadata and Interfederation. The Operator may process and publish organisational, contact and technical metadata necessary for Federation and approved Interfederation operation, subject to Schedule D.

11. Security and incident response

11.1 Minimum controls. Participants shall maintain proportionate governance, access control, patching, logging, monitoring, backup, recovery, vulnerability and personnel controls for registered Entities and services.

11.2 Security contacts. Security contacts shall be reachable and authorised to coordinate action. Participants shall adopt Sirtfi or a successor security Profile where required for eduGAIN or a Participating Service.

11.3 Notification. A participant shall notify the Operator without undue delay of an incident that may affect Federation security, trustworthiness, personal data, metadata or another participant.

11.4 Cooperation. Participants shall preserve relevant evidence, contain harm, provide accurate updates and cooperate in remediation and post-incident review.

11.5 Confidentiality. Incident information shall be shared on a need-to-know basis, without preventing lawful reporting, member accountability or necessary protective action.

12. Interfederation and eduGAIN

12.1 Participation. eduID.ng may participate in eduGAIN and other arrangements approved under this Policy to enable access across organisational and national boundaries.

12.2 Metadata export. The Operator may export eligible Entity metadata in accordance with the applicable Profile, member election and community-approved rules.

12.3 External policies. Members acknowledge that Interfederation may involve entities subject to other laws and federation policies. Participation does not create a general guarantee by eduID.ng regarding an external entity.

12.4 Entity categories. Research & Scholarship, Code of Conduct, Sirtfi and other recognised categories or frameworks may be adopted through Profiles with stated compliance criteria.

13. Fees and sustainability

13.1 Sustainability plan. The Council shall propose a transparent sustainability plan covering core federation operations and integrated services for consideration by the AoM.

13.2 Charges. Fees or charges must be approved under the delegated financial authority, published in advance and applied fairly to the relevant membership or service class.

13.3 No retrospective charge. A new charge shall not apply retrospectively and shall take effect only after reasonable notice.

14. Liability

14.1 Distributed responsibility. Each participant is responsible for the systems, identities, Attributes, services, decisions, acts and omissions under its control.

14.2 No warranty. Federation services are provided on a reasonable-efforts and as-available basis. No participant guarantees uninterrupted or error-free operation unless expressly stated in a service agreement.

14.3 Exclusion. To the extent permitted by law, the Operator, Council, AoM and Members shall not be liable solely by reason of Federation participation for indirect or consequential loss caused by another participant or external federation entity.

14.4 Exceptions. Nothing in this Policy excludes liability that cannot lawfully be excluded, including liability arising from fraud, wilful misconduct or other liability imposed by applicable law.

14.5 Separate agreements. Participants may agree to additional service levels, warranties, indemnities or liability terms for a Participating Service. Those terms apply only to the relevant parties and service.

15. Suspension, termination, withdrawal and appeal

15.1 Emergency suspension. The Operator may temporarily suspend an Entity, Profile or service connection where reasonably necessary to address an immediate security, privacy, legal or operational risk.

15.2 Safeguards. Suspension shall be proportionate and documented. The affected participant shall be notified promptly, given reasons to the extent lawful and safe, and offered remediation and review.

15.3 Membership termination. Only the Council may terminate membership, following notice, a reasonable opportunity to remedy or respond, and consideration of proportionality. The AoM shall hear any final appeal.

15.4 Withdrawal. A Member may withdraw on written notice. Withdrawal does not remove accrued obligations and shall include orderly removal of metadata, access and service dependencies.

15.5 Appeal. An adversely affected applicant or participant may request reconsideration and appeal in accordance with Schedule B.

16. Disputes and jurisdiction

16.1 Good-faith resolution. A dispute shall first be referred to authorised representatives for good-faith negotiation.

16.2 Mediation. If unresolved within 15 business days, either party may request facilitated resolution or mediation arranged by the Council, subject to conflicts of interest.

16.3 Court proceedings. If unresolved within 30 business days after mediation is requested, a party may bring proceedings before a court of competent jurisdiction in the Federal Republic of Nigeria.

16.4 Urgent relief. Nothing prevents urgent protective or injunctive relief where delay would cause material harm.

17. Amendment and change control

17.1 Core Policy. Amendment of the Core Policy or reserved constitutional provisions requires member consultation and approval by at least two-thirds of votes cast at a quorate AoM meeting.

17.2 Schedules. A Schedule may be amended by the Council after proportionate consultation, except a reserved provision or Schedule A change affecting AoM authority, representation or accountability, which requires AoM approval.

17.3 Profiles and Procedures. The Council may approve or delegate approval of Profiles and Procedures following technical review and appropriate notice.

17.4 Urgent changes. The Operator may implement a temporary urgent security or continuity change, subject to prompt documentation, Council review and a defined expiry or formal approval.

17.5 Notice. Unless urgency requires otherwise, material changes shall be communicated at least 30 days before taking effect. A longer period shall be used where implementation effort is significant.

18. Continuity and operator transition

18.1 Continuity plan. The Operator shall maintain and test a proportionate continuity and recovery plan for critical federation services.

18.2 Operator withdrawal. The Operator shall give at least 12 months' notice of intended withdrawal unless prevented by circumstances beyond its reasonable control.

18.3 Transition. The AoM, acting on Council recommendation, appoints a successor Operator. The outgoing Operator shall support orderly transfer of authorised records, metadata, configurations, keys where lawful and appropriate, documentation, service dependencies and operational knowledge.

18.4 Community assets. Federation policy records, registers, community decisions and operational materials produced specifically for eduID.ng shall be preserved for Federation continuity, subject to law, licences and third-party rights.

19. Transitional provisions

19.1 Existing members and entities. Existing memberships and registrations continue, subject to a compliance refresh within six months after the effective date.

19.2 Governance transition. The existing governance bodies continue on an interim basis only to implement the transition. Elections or confirmations under Schedule A shall occur within 90 days after the effective date.

19.3 Existing instruments. Existing procedures remain in force to the extent consistent with this Policy until replaced or withdrawn.

19.4 Effective date. This Policy takes effect on the date approved by the AoM or on a later date specified in its resolution.

SCHEDULE A - GOVERNANCE CONSTITUTION

A1. Assembly of Members

A1.1 Composition. Each full Federation Member belongs to the AoM and appoints one authorised voting representative and one alternate.

A1.2 Functions. The AoM approves the Core Policy and reserved matters; elects or confirms Council members; receives annual reports; approves strategic direction; delegates work; and determines appeals reserved to it.

A1.3 Meetings. The AoM shall meet at least annually. A special meeting may be called by the Council or on written request of at least one-fifth of full Members.

A1.4 Notice. Ordinary meetings require at least 21 days' notice and special meetings at least 10 days, unless urgent action is unanimously accepted by those present.

A1.5 Quorum. Quorum is one-third of full Members, rounded up. If quorum is not achieved, a reconvened meeting on the same agenda may proceed after at least seven days' notice with those attending, except for reserved constitutional matters.

A1.6 Voting. Each full Member has one vote. Ordinary decisions require a simple majority of votes cast. Core Policy, removal of an elected Council member, change of Operator and other reserved matters require two-thirds of votes cast at a quorate meeting.

A1.7 Electronic action. Meetings and voting may take place electronically using a method that reasonably verifies participation and records the decision.

A1.8 Proxies. A representative may hold no more than two written proxies.

A2. Federation Council

Composition:

- Chair, elected by the AoM;
- Vice-Chair, elected by the AoM;
- four representatives elected from full Members, with reasonable balance across institution types and geography;
- one representative of participating Service Providers or community services, elected by the AoM; and
- Technical Committee Coordinator, ex officio with voting rights.

The Federation Coordinator attends as the Operator's representative and Council Secretary but does not vote. The Council may invite WACREN, regulators, sector bodies or other advisers as non-voting observers.

A2.1 Term. Elected members serve two-year terms and may serve no more than two consecutive full terms in the same office.

A2.2 Functions. The Council oversees strategy, policy implementation, risk, security, sustainability, services, performance and compliance; approves matters delegated by this Policy; and reports to the AoM.

A2.3 Limit. The Council shall not amend AoM reserved matters or convert delegated authority into permanent independent authority.

A2.4 Meetings. The Council meets at least quarterly. Quorum is a majority of voting members. Decisions are by simple majority; the Chair has a casting vote only after each voting member has voted.

A2.5 Vacancy. The Council may appoint an eligible interim member until the next AoM meeting, except that a vacancy in the Chair shall be filled by the Vice-Chair.

A2.6 Removal. The AoM may remove an elected member for misconduct, persistent non-participation, loss of eligibility or serious conflict, after notice and an opportunity to respond.

A2.7 Reporting. Minutes, decisions and an annual report shall be made available to Members, with lawful redactions for security, privacy, legal privilege or commercial confidentiality.

A3. Conflicts and conduct

A3.1 Declaration. A person participating in governance shall declare actual, potential or perceived conflicts of interest.

A3.2 Management. The Chair, or Vice-Chair where the Chair is conflicted, shall determine proportionate management, including disclosure, recusal or non-receipt of restricted information.

A3.3 Conduct. Participants shall act respectfully, in good faith and in the interests of the Federation community, protect confidential information and avoid misuse of position.

A4. Working Groups and Technical Committee

A4.1 Terms of reference. Each group shall have written scope, deliverables, membership, chair, reporting line, duration and decision or recommendation authority.

A4.2 Openness. Participation should be open to appropriately qualified community members unless confidentiality, manageability or required expertise justifies restriction.

A4.3 PRWG. The Policy Review Working Group completes the mandate delegated by the AoM when its recommendation and draft are submitted and the AoM determines the matter, unless the AoM extends its mandate.

A4.4 Technical Committee. The AoM confirms a Technical Committee Coordinator. The Council approves other members following an open call, on recommendation of the Coordinator and Operator. The Committee shall have at least five members and report at least quarterly.

SCHEDULE B - MEMBERSHIP AND PARTICIPATION

B1. Participation classes

Class	Position
Full Member	Eligible Nigerian research or education organisation operating or sponsoring at least one Entity; voting AoM membership.
Service Provider Member	Organisation primarily participating to provide one or more services; may elect the service representative but does not obtain a second vote if already a Full Member.
Affiliate	Public-interest, sector, infrastructure or partner organisation approved for defined participation; non-voting unless separately eligible as a Full Member.
Registered Service	A service approved under Schedule E; registration alone does not confer organisational membership.

B2. Application and review

- signed acceptance of this Policy by an authorised representative;
- evidence of legal identity and eligibility;
- required administrative, technical, security and privacy contacts;
- description of intended Entities, Profiles and services;
- technical and security readiness evidence;

- Identity Management Practice Statement where acting as a Home Organisation; and
- any additional information reasonably required for risk and compliance assessment.

B2.1 Timeframe. The Operator should acknowledge a complete application within five business days and decide or refer it within 20 business days.

B2.2 Reasons. A refusal or conditional approval shall give reasons and identify any available remediation or reconsideration route.

B2.3 Reconsideration. An applicant may seek Operator reconsideration within 15 business days and appeal to the Council within a further 15 business days.

B3. Annual validation

Each Member shall annually validate its contacts, eligibility, Entities, adopted Profiles, service dependencies and material compliance information. Failure to validate after notice may result in restricted metadata export or suspension.

SCHEDULE C - TECHNICAL AND TRUST PROFILES

C1. Profile suite

Profile	Purpose
Metadata Registration Practice Statement	How entities are registered, validated, published, signed, changed and removed; includes the authoritative edulD.ng registration authority.
SAML WebSSO Profile	SAML entity, endpoint, certificate, identifier and interoperability requirements.
OpenID Connect Federation Profile	Requirements applicable only when edulD.ng supports OIDC federation in production.
Attribute Profile	Approved schema, identifiers, release expectations and semantic definitions.
Assurance Profile	Identity proofing, credential, authentication and lifecycle assurance requirements.
Security and Incident Profile	Minimum controls, security contacts, Sirtfi requirements and incident coordination.
Entity Category Profile	Criteria and declarations for Research & Scholarship, Code of Conduct and other adopted categories.
Service Profiles	Technical and trust requirements for individual integrated services.

C2. Profile adoption

C2.1 Review. A proposed Profile shall undergo Technical Committee review, security and privacy assessment, implementability testing and proportionate member consultation.

C2.2 Approval. The Council approves Profiles unless it has delegated approval of a defined technical class to the Technical Committee, subject to Council ratification.

C2.3 Versioning. A Profile shall state its version, authority, effective date, transition period, conformance method and consequences of non-conformance.

C2.4 Protocol neutrality. The Core Policy does not require a particular protocol. Only production-supported and published Profiles create technical obligations.

SCHEDULE D - PRIVACY AND DATA PROTECTION

D1. Required controls

- a documented purpose and lawful basis for each relevant processing activity;

- privacy information accessible before or at first federated use;
- Attribute minimisation and periodic review of requested Attributes;
- access controls and confidentiality for administrative and security contacts;
- retention periods for authentication, metadata, support and security logs;
- procedures for data-subject rights and complaints;
- personal-data breach assessment, notification and cooperation;
- appropriate processor or data-sharing terms where required; and
- assessment of international transfers or access where Interfederation processing requires it.

D2. Federation logs

D2.1 Purpose. The Operator may retain proportionate technical and administrative logs for security, troubleshooting, audit, service measurement and legal compliance.

D2.2 Retention. Default retention periods shall be documented in a public or member-accessible retention schedule and reviewed at least annually.

D2.3 Disclosure. Logs shall be disclosed only where authorised, necessary and proportionate, including incident response, legal obligation and properly governed service support.

SCHEDULE E - OPERATIONS AND SERVICE INTEGRATION

E1. Operational controls

- documented service ownership and accountable contacts;
- change, release and configuration management;
- monitoring, backup, recovery and dependency management;
- certificate, key and secret lifecycle management;
- incident and problem management;
- capacity and availability objectives proportionate to service criticality;
- member communications and status information; and
- annual continuity and supplier-risk review.

E2. Service onboarding

E2.1 Proposal. A service sponsor shall submit a service description, community value case, owner and provider, target users, technical architecture, data flows, Attribute needs, security and privacy assessment, support model, costs, sustainability and exit plan.

E2.2 Assessment. The Operator and Technical Committee assess technical readiness, interoperability, security, privacy, operational capacity and policy fit. Material financial or governance commitments require Council approval.

E2.3 Schedule. Before production onboarding, each service shall have an approved schedule stating eligibility, roles, trust and assurance, data processing, support, service objectives, fees, suspension, termination, portability and exit.

E2.4 Pilot. A time-limited pilot may be authorised with defined participants, safeguards, success criteria and end date. A pilot does not create an entitlement to production operation.

E2.5 Review. Each production service shall be reviewed at least annually for value, adoption, security, privacy, performance, cost and sustainability.

E3. Service boundaries

E3.1 Federated access. A service using eduID.ng authentication remains governed by its own service terms in addition to applicable Federation Policy Instruments.

E3.2 Hosted identity. A hosted IdP or identity-as-a-service offering shall define allocation of identity lifecycle responsibilities between the Home Organisation and provider; the Home Organisation remains accountable for authoritative identity decisions.

E3.3 geteduroam onboarding. geteduroam shall be treated as a Participating Service under this Schedule, not as a Federation Technology Profile or a substitute for eduroam participation. Its service schedule shall cover institutional eligibility, identity proofing, credential or certificate issuance, device-profile delivery, revocation, support, logging, privacy, security, suspension and exit.

E3.3.1 edulD.ng scope. edulD.ng may authenticate an End User, confirm institutional affiliation or entitlement, and provide approved identity information needed to initiate onboarding. It does not make the final eduroam network-access decision.

E3.3.2 Onboarding service operator. The geteduroam service operator is responsible for secure onboarding, approved device configuration, protection and lifecycle management of any credentials or certificates it issues, appropriate logging, user support and revocation capabilities.

E3.3.3 Home Organisation. The Home Organisation remains responsible for the accuracy and lifecycle of its users' identities, affiliations and entitlements and for promptly withdrawing eligibility when the underlying relationship changes.

E3.3.4 eduroam infrastructure. The eduroam Identity Provider remains responsible for authenticating the user through the applicable RADIUS or RadSec infrastructure. The national eduroam operator remains responsible for national roaming infrastructure, realm routing, operational coordination and compliance with applicable eduroam requirements.

E3.3.5 Visited institution. An institution providing visited eduroam access remains responsible for its wireless network, local access controls, network-use requirements and operational or abuse handling duties under the applicable eduroam policy.

E3.3.6 Separate eligibility and suspension. Approval, restriction or suspension under edulD.ng or geteduroam does not automatically determine an institution's eduroam status, and an eduroam action does not automatically terminate edulD.ng membership. Where a shared risk affects both services, the responsible operators shall coordinate proportionate action under their respective policies.

E3.4 Publishing and repositories. Publishing, repository, PID or discovery services may use edulD.ng for authentication and roles but shall define their own content, editorial, preservation, rights and service governance.

E4. Exit and portability

E4.1 Exit plan. Every material service shall maintain a documented exit plan covering notice, data return or deletion, identity and access revocation, dependency removal, records, communications and continuity alternatives.

E4.2 Provider change. A provider change shall be governed as a material service change and shall protect Members and End Users from avoidable lock-in or loss of authorised data.

APPROVAL RECORD

Mandate	Mandate: PRWG established by the Assembly of Members at its inaugural convening, 20 May 2026
PRWG recommendation date	17 September 2026
Member ratification period	21-25 September 2026 (electronic vote, closed 18:00 WAT)
AoM resolution	Ratified unanimously, 25 September 2026

Votes	23 in favour, 0 against, 0 abstentions. Turnout: 23 of 38 member representatives (60.5%); 15 representatives did not vote. Quorum and two-thirds threshold met.
Clerical correction	Proposed effective date on cover page corrected from 28 September 2028 to 28 September 2026.
Effective date	28 September 2026
Next scheduled review	No later than 28 September 2029

End of eduID.ng Federation Policy v2.0