unicef | for every child

TERMS OF REFERENCE

ICT Individual Consultant in Child Online Protection (technical support to MINICT)

(National candidates only)

CONTRACT MODALITY	Individual Consultancy
DUTY STATION	Kigali, Rwanda-based, office-based at the Ministry of ICT and Innovation (MINICT), with approved missions within Rwanda
DURATION OF CONTRACT	11.5 months

Purpose of Assignment

The Ministry of ICT and Innovation (MINICT) is the Government of Rwanda's lead institution for Child Online Protection (COP) and for the safe and responsible use of digital technologies by children and young people. Children and young people in Rwanda are increasingly accessing social media platforms, online gaming, messaging and video-sharing services and generative Artificial Intelligence (AI) tools, and the associated risks — online grooming and sexual exploitation, cyberbullying, exposure to age-inappropriate content, excessive use, commercial profiling of minors and AI-generated abuse material — are evolving rapidly.

Under the Rwanda–UNICEF Programme of Cooperation 2025–2029, MINICT and UNICEF signed a 2026–2027 Multi-Year Work Plan on 27 August 2026 (1 July 2026 – 31 December 2027) comprising twelve activities under Child Protection Outputs 1.1 and 1.2 and Education Output 1.3: a national digital parenting programme (1.1.1); a multi-channel national behaviour-change campaign on child online safety (1.1.2); integration of child online protection and digital literacy into curricula (1.1.3); training modules for teachers, social workers and community-based child protection actors (1.1.4); a Child Online Protection Hackathon (1.1.5); inter-Ministry coordination to implement the COP research recommendations (1.2.1); a national child online protection regulatory framework, including standards on age verification, Internet Service Provider (ISP) accountability and content moderation (1.2.2); high-level advocacy (1.2.3); capacity building of law enforcement, prosecutors and the judiciary on digital evidence and online crimes affecting children (1.2.4); and teacher capacity building and digital literacy, AI and ICT skills for young people through the Ingazi platform (1.3.1–1.3.3). MINICT's accelerated implementation plan of 21 September 2026 requires all activities to start before 30 November 2026.

To deliver this Work Plan, MINICT has requested dedicated technical support with complementary profiles — child online protection, legal and ICT — to work as an integrated team under Activity 1.2.1. This deliverable-based consultancy provides the ICT expertise: the monitoring and analysis of harmful content and emerging online risks, the assessment of the safety features and practices of digital platforms and AI-enabled services, the technical criteria for content classification and age-rating, the design of secure monitoring, reporting and referral tools, and the technical content of the regulatory framework, the awareness campaign and the capacity-building activities.

The consultant will produce defined, reviewable technical products and will not replace staff functions, provide day-to-day operational support, exercise supervisory authority, represent UNICEF or MINICT in decision-making, or manage UNICEF resources.

Scope of Work

Objective: Provide time-bound ICT technical expertise to MINICT and UNICEF to plan, implement and monitor the technical components of the 2026–2027 MINICT–UNICEF Child Online Protection Work Plan, and to translate technical findings into evidence for policy, regulatory and programmatic action.

The consultant will be based at MINICT, will work day-to-day with the MINICT Child Online Protection focal point and will report to the UNICEF Contract Manager. The consultancy will focus on the following areas:

1. **Coordination support (Activity 1.2.1):** Support the MINICT focal point in coordinating the implementation of the COP research recommendations with NCDA, MIGEPROF, MINEDUC/REB and child-focused civil society organisations; maintain the tracking of recommendations and action points; prepare agendas, minutes and follow-up of the inter-ministerial technical working group; and map and strengthen referral pathways for online harms.

2. **Platform safety assessment:** Assess the safety features and technical safeguards of the platforms and AI-enabled services used by children in Rwanda — age assurance, parental controls, privacy defaults, recommender systems, AI chatbots, content filters, reporting and content moderation practices — and identify opportunities to strengthen child safety online.

3. **Content classification and age-rating:** Develop, with the legal technical support, the technical criteria and framework for the identification, categorisation, classification and age-rating of content accessible to children, as an input to the national regulatory framework (Activity 1.2.2).

4. **Technical standards for the regulatory framework (Activity 1.2.2):** Provide the technical input to the national Child Online Protection regulatory framework — age assurance, content moderation, age-rating, platform accountability, privacy-by-design, parental controls and child-safe reporting mechanisms — and support the technical sessions of the stakeholder consultations with RURA, NCSA, RISA, internet service providers and online platforms.

5. **Monitoring, reporting and referral systems:** Design and support the implementation of secure systems, tools and workflows for the monitoring, documentation, reporting, referral and follow-up of harmful online content and online risks affecting children, aligned with the national child protection case-management and referral system and the child helpline, applying data protection by design.

6. **Technical content for awareness and capacity building (Activities 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.3.1): Provide** and review the technical content of the digital parenting programme, the national awareness campaign (including the animated step-by-step guide on parental controls for the devices children use), the curriculum materials and the training modules for teachers and social workers, on the safe and responsible use of digital technologies, social media, online gaming and AI tools.

7. **Justice-sector capacity building and the Hackathon (Activities 1.2.4 and 1.1.5):** Contribute the technical content on digital evidence and online harms to the training manuals and SOPs for law enforcement, prosecutors and the judiciary and co-facilitate the technical sessions; and provide technical mentoring and the technical parameters for solutions developed at the Child Online Protection Hackathon.

8. **Analysis and reporting:** Monitor and analyse harmful and age-inappropriate content and emerging online risks affecting children across social media, messaging, gaming, video-sharing and AI-enabled services; analyse platform practices and digital trends; and produce periodic analytical reports with evidence-based recommendations for policy, regulation, awareness and programme implementation.

This consultancy is a technical advisory role focused on systems, standards, analysis and technical content. The consultant will not provide direct services to children, undertake case management, interview children, or have unsupervised interpersonal contact with children. The consultant will not collect, store or process personally identifiable information of children or handle individual cases or reports; any report, case or item of harmful content involving an identifiable child encountered during the assignment will be referred immediately through the authorised MINICT, NCDA and law-enforcement channels. Technical monitoring will be conducted at the level of platforms, practices, trends and aggregated evidence.

Work Assignments Overview	Deliverables/Outputs	Delivery deadline to complete the deliverable
Inception and joint work plan	Deliverable #1 Accepted inception package comprising desk review of the COP research, the Work Plan and relevant national instruments; landscape of platforms and services used by children in Rwanda; consultancy deliverable workplan; and the joint work plan of the integrated technical team agreed with the MINICT focal point.	29 Dec 2026
Technical content for the campaign and digital parenting programme	Deliverable #2 Accepted technical content package: technical review and device-specific content of the animated parental-controls guide and campaign materials (Activity 1.1.2); technical content of the digital parenting materials (1.1.1); and technical input to the curriculum materials and teacher/social-worker training modules (1.1.3, 1.1.4, 1.3.1), with a review log of comments and resolutions. Products must promote children's agency, digital literacy and help-seeking, not fear-based messaging.	15 Feb 2027
Platform safety assessment	Deliverable #3 Accepted assessment report on the safety features and technical safeguards of the main platforms and AI-enabled services used by children in Rwanda (age assurance, parental controls, privacy defaults, recommender systems, AI chatbots, content filters, reporting and moderation), with prioritised technical recommendations and a Government and industry engagement plan.	15 Mar 2027
Content classification and age-rating framework	Deliverable #4 Accepted technical framework and criteria for the identification, categorisation, classification and age-rating of content accessible to children, developed with the legal technical support and validated by MINICT, as an input to the regulatory framework.	28 Feb 2027
Technical standards and consultations for the regulatory framework	Deliverable #5 Accepted technical standards chapter for the national COP regulatory framework (age assurance, content moderation, platform accountability, privacy-by-design,	15 Mar 2027

	parental controls, child-safe reporting); technical sessions delivered in the stakeholder consultations with RURA, NCSA, RISA, ISPs and platforms, with session records and a comments-and-response log.	
Harmful-content monitoring, reporting and referral system	Deliverable #6 Accepted system package: functional and data-protection specification; workflow and SOP for monitoring, documentation, reporting, referral and follow-up of harmful online content aligned with the national referral system and the child helpline; working prototype or configured tool; and orientation of the MINICT and NCDA focal points, with records.	15 Jun 2027
Technical content for justice-sector training and the Hackathon	Deliverable #7 Accepted technical modules on digital evidence and online harms for the law-enforcement, prosecution and judiciary training manuals/SOPs (Activity 1.2.4) and co-facilitation of the technical sessions, with participant records; and technical mentoring input and technical parameters for Hackathon solutions (Activity 1.1.5), with a mentoring note.	15 Jun 2027
Online-risk analysis and periodic reporting	Deliverable #8 Two accepted analytical reports on harmful content, emerging online risks, platform practices and digital trends affecting children, with evidence-based recommendations: the first by 28 Feb 2027 and the second by 15 October 2027; plus monthly technical progress inputs to MINICT and UNICEF.	First report: 28 Feb 2027 Second report: 15 Nov 2027
Final results and handover	Deliverable #9 Accepted handover package: consolidated results report; deliverable/evidence index including completed, pending and recommended follow-up actions; technical recommendations for the 2027 activities; organised handover files and tools transferred to MINICT.	30 Nov 2027

Payment Schedule:

Payment will be made on submission and acceptance of deliverables. UNICEF reserves the right to withhold payment in case the deliverables submitted are not up to the required standard or in case of delays in submitting the deliverables on the part of the consultant.

Important Notes

- Individuals engaged under a consultancy or individual contract will not be considered "staff members" under the Staff Regulations and Rules of the United Nations and UNICEF's policies and procedures and will not be entitled to benefits provided therein (such as leave entitlements and medical insurance coverage). Their conditions of service will be governed by their contract and the General Conditions of Contracts for the Services of Consultants and Individual Contractors. Consultants and individual contractors are responsible for determining their tax liabilities and for the payment of any taxes and/or duties, in accordance with local or other applicable laws.
- Contracts are conditional upon the selected candidate's willingness to comply with any current or future vaccination requirements that may be established by UNICEF, where applicable. Failure to comply with applicable vaccination requirements, where required and without an approved medical exemption by UNICEF, may result in the withdrawal of the consultancy offer or termination of the contract in accordance with the General Terms and Conditions of Contract.
- UNICEF offers reasonable accommodation for consultants with disabilities. This may include, for example, accessible software, travel assistance for missions or personal attendants. We encourage you to disclose your disability during your application in case you need reasonable accommodation during the selection process and afterwards in your assignment.

QUALIFICATIONS / SPECIALIZED KNOWLEDGE / EXPERIENCE/ COMPETENCIES (CORE/TECHNICAL/FUNCTIONAL) / LANGUAGE SKILLS REQUIRED FOR THE ASSIGNMENT

Minimum requirements:

Education:

- Advanced university degree (Bachelor's or higher) in one of the following fields is required: I Information and Communication Technology, Computer Science, Information Systems, Software Engineering, Cybersecurity, Data Science, Artificial Intelligence or another closely related ICT field. A postgraduate qualification or professional certification in cybersecurity, online safety, data analytics, AI, digital forensics or child.

Work Experience:

- At least five years of progressively responsible professional experience in ICT, computer science, information systems, cybersecurity, data analysis, artificial intelligence or another relevant technology field, with demonstrated exposure to online safety, digital platforms or child online protection.

Knowledge/Expertise/Skills:

- Demonstrated technical knowledge of social media platforms, online gaming, messaging and video-sharing services, AI-enabled tools and the online risks affecting children.
- Experience assessing or configuring platform safety features, including age assurance, parental controls, privacy settings, recommender systems, AI chatbots, content filters and reporting mechanisms.
- Experience designing or supporting digital monitoring, data collection, reporting, referral or case-tracking tools, with strong attention to data protection, information security and the safe handling of sensitive information.

- Ability to analyse technical evidence and communicate findings clearly to non-technical audiences for policy, regulatory and programmatic action.
- Ability to work in a fast-paced environment, to meet deadlines, and to take initiative to troubleshoot and solve problems before they arise.

Language Requirements:

- Fluency in English (verbal and written) required.
- Fluency in Kinyarwanda (verbal and written) required.
- Knowledge of French is an asset.

Desirables:

- Experience working with government institutions, regulators, technology companies, online platforms, schools, civil society organisations or development partners in Rwanda.
- Familiarity with child rights, child safeguarding and online safety standards, and with UNICEF and UN policies and practices including protection from sexual exploitation and abuse (PSEA).
- Experience developing or reviewing child-friendly awareness, digital-literacy or training materials on the safe use of digital technologies.
- Knowledge of content classification, age-rating, content moderation or platform governance.
- Strong analytical, research, coordination, communication and report-writing skills, and the ability to work independently and within a multidisciplinary team.

Technical Proposal:

- A concise proposal describing the candidate's understanding of the assignment, methodology, deliverable workplan, data-protection and safeguarding approach and risk management.