TAF

TELECOMMUNICATIONS AUTHORITY OF FIJI

Level 2, LICI House, 11 Butt Street, Suva. | G.P.O Box 13413, Suva, Fiji | Phone: (679) 3310101 | Fax: (679) 3310110 | www.taf.org.fj | contact@taf.org.fj

05 November 2026

DETERMINATION 01/2026 - RESTRICTION OF ACCESS TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE MATERIAL ("CSEAM")

Recitals

WHEREAS:

A. The Telecommunications Authority of Fiji ("the Authority") is established under the Telecommunications Act 2008 ("the Act") and is responsible for regulating telecommunications services in Fiji;

B. Section 3 of the Act requires the Authority to exercise its functions in furtherance of the objectives set out therein, including providing and promoting appropriate consumer protection and other safeguards in relation to telecommunications services where market forces are insufficient;

C. Section 18(1) of the Act empowers the Authority to make determinations relating to a Licensee's obligations upon its own motion, where it has reason to believe a determination is necessary;

D. Section 62A of the Juveniles Act 1973 makes it an offence for any person to record, reproduce, place onto, view, access, publish, solicit, distribute, traffic in, or sell material depicting a juvenile, or a person appearing to be a juvenile, engaged in sexually explicit conduct, and defines "records" to include telecommunications and internet-based media;

E. Sections 72 and 73 of the Act impose a best-endeavors obligation on the Authority and a corresponding best-endeavors obligation on Licensees respectively, to prevent Fiji's telecommunications networks from being used in the commission of offences in Fiji, with protection from liability for acts done in good faith under a direction given pursuant to Section 72 of the Act;

F. Section 21 of the Act requires the Authority, in making a determination, to consider the effect of the determination on users and Licensees and whether the reasonably anticipated benefits to users outweigh the regulatory burden reasonably anticipated to be placed on Licensees;

G. The Cabinet of Fiji has established the National Taskforce to Understand the Societal Risks of Pornography Use in Fiji and Provide Recommendations to Address it ("the National Taskforce"), comprising government agencies and key stakeholders, to

coordinate a whole-of-government response to the societal impacts of pornography, the first workstream of which is to combat online child sexual exploitation and abuse material; the National Taskforce includes three working groups, one of which is Working Group 3: Industry and Technology Response ("WG3"), which brings together the Authority, Licensees providing an Internet Access Service, and the Fiji Police Force to coordinate the technical and operational response;

H. The Fiji Police Force maintains access to a secure INTERPOL system used to access a number of INTERPOL law-enforcement databases; access to the IWOL database specifically requires the prior execution of an agreement between the Fiji Police Force and each Licensee ("the IWOL Agreement"), following which the precise technical means by which Reference Data will be made available to Licensees will be established between the Fiji Police Force and the relevant Licensee;

I. INTERPOL administers the "Worst of" List ("IWOL"), which identifies online resources containing child sexual exploitation and abuse material through a rigorous multi-officer verification process requiring that:

   i. the material depicts a real child who is prepubescent or in the early stages of puberty and perceived to be under 13 years of age, and depicts sexual activity involving the child or focuses on the child's genital or anal region;

   ii. the material is accepted as meeting the IWOL criteria by two independent specialised officers from INTERPOL member countries or INTERPOL's Crimes Against Children (CAC) Unit; and

   iii. the material is confirmed by a third officer from the INTERPOL CAC Unit, and only when all of these requirements are met may a qualifying domain be included in the IWOL;

   material classified in accordance with this process, consistent with INTERPOL's published Baseline Criteria, is treated as illegal in all 196 INTERPOL member countries[1];

J. On 12 June 2026, the Authority communicated with Licensees regarding its intended engagement with the IWOL programme, affording Licensees advance notice to prepare for the requirements ultimately imposed by this Determination;

K. On 6 August 2026, the Authority issued a Notice of Proposed Determination to Licensees providing an Internet Access Service, in accordance with Sections 18(3) and 22 of the Act, inviting written submissions within 14 days;

L. The Authority received written submissions from three Licensees providing an Internet Access Service, from 17 August to 25 September 2026, and has had regard to those submissions in accordance with Section 22(d) of the Act;

[1] see INTERPOL, "Blocking and Categorizing Content", available at: https://www.interpol.int/Crimes/Crimes against-children/Blocking-and-categorizing-content

M. Having considered those submissions, the Authority has decided to make this Determination to address the operational, technical and legal matters raised during consultation;

N. Written reasons for this Determination, addressing the matters raised in consultation and the Authority's consideration under Section 21 of the Act, are set out at Schedule 1, in accordance with Sections 18(3)(c) and 22(e) of the Act.

Roles and Responsibilities Framework

For clarity, the demarcated roles and responsibilities under this Determination are as follows:

(a) The Authority determines the obligations of Licensees and the safeguards applicable under this Determination;

(b) The Fiji Police Force, in its capacity as Fiji's INTERPOL National Central Bureau, and any other Authorised Source, own the law-enforcement reference-data relationship, including the facilitation of the receipt, governance and transmission of Reference Data (including each Update) to Licensees, and, together with the Authority, the review and correction of any Reference Data Error;

(c) INTERPOL or the relevant Authorised Source owns the underlying CSEAM classification and verification process, which is conducted exclusively by that source in accordance with its established procedures;

(d) Licensees are responsible for implementing reasonable and proportionate Technical Measures, and each Update, in accordance with this Determination, acting in good faith reliance on the Reference Data supplied by the Authorised Source, and for promptly correcting any Implementation Error; and

(e) WG3 coordinates implementation under this Determination but does not exercise the Authority's regulatory powers and has no authority to determine the validity of CSEAM classifications.

NOW THEREFORE, pursuant to Section 18 of the Act, the Authority determines as follows:

Part 1 – Preliminary

1. Short Title

This Determination may be cited as the CSEAM Access Restriction Determination 2026.

2. Commencement

This Determination comes into force on the date of issuance.

3. Application

This Determination applies to every Licensee that provides an Internet Access Service in Fiji.

4. Definitions

In this Determination, unless the context otherwise requires:

"**Authorised Source**" means the Fiji Police Force, in its capacity as Fiji's INTERPOL National Central Bureau, or any international or national law-enforcement reference source approved by the Authority for the purposes of this Determination, following consultation with the Fiji Police Force and, where appropriate, the National Taskforce;

"**CSEAM**" means online child sexual exploitation and abuse material, including material of the kind described in Section 62A of the Juveniles Act 1973;

"**Implementation Error**" means any restriction, or any failure to restrict or to remove a restriction, that results from a Licensee's own configuration, deployment, operation or maintenance of Technical Measures (including a restriction extending beyond the online resources identified in the Reference Data, or a failure to apply an Update within the applicable timeframe under clause 12), as distinguished from a Reference Data Error;

"**Internet Access Service**" has the meaning given in the Act;

"**IWOL**" means the INTERPOL "Worst of" List, or any successor or equivalent list maintained by INTERPOL, identifying online resources containing child sexual exploitation and abuse material that have been verified in accordance with INTERPOL's established classification and multi-officer verification procedures;

"**IWOL Agreement**" means the agreement, by whatever name styled, between a Licensee and the Fiji Police Force (or such other Authorised Source as applicable) governing the receipt of Reference Data derived from the IWOL, together with any related arrangement, however implemented, for connecting to, or receiving Reference Data from, the system through which the IWOL is made available;

"**Landing Page**" means the informational page referred to in clause 28, displaying at a minimum the content set out in Schedule 2;

"**Licensee**" means a person (including a body corporate) licensed under the Act to provide an Internet Access Service in Fiji;
"**National Taskforce**" means the National Taskforce to Understand the Societal Risks of Pornography Use in Fiji and Provide Recommendations to Address it, established by Cabinet;

"**Reference Data**" means official data identifying online resources associated with CSEAM, provided by, or through, an Authorised Source, including data comprised in or derived from the IWOL, as updated from time to time by way of Updates;

"**Reference Data Error**" means an error in the Reference Data as supplied by the Authorised Source, including the inclusion of a legitimate online resource, as distinguished from an Implementation Error;

"**Technical Measures**" means reasonable and proportionate technical measures, undertaken in good faith, to restrict access to online resources identified in the Reference Data, including domain, URL, IP address or protocol-based controls, while minimising restriction of lawful content;

"**Update**" means any addition to, amendment of, or removal from the Reference Data made by the Authorised Source and communicated to Licensees; and

"**WG3**" means Working Group 3 – Industry and Technology Response, established under the National Taskforce, comprising the Authority, Licensees providing an Internet Access Service, and the Fiji Police Force.

Part 2 – Core Obligation

5. Every Licensee shall implement reasonable and proportionate Technical Measures to restrict access to online resources identified in the Reference Data, as updated from time to time.

6. The obligation in clause 5 is made pursuant to Section 18 of the Act. It applies automatically upon each Update transmitted in accordance with Part 3, whether an addition, an amendment or a removal, without the need for a further direction or notice in respect of any individual addition to, amendment of, or removal from, the Reference Data.

7. Nothing in this Determination requires a Licensee to decrypt, intercept, or inspect the content of any encrypted communication. A Licensee is not in breach of clause 5 solely because its Technical Measures do not restrict access achieved through encrypted tunnels, virtual private networks, Tor, content delivery networks, or other circumvention or shared-hosting technologies, provided the Licensee has used reasonable efforts to implement Technical Measures that are reasonable and proportionate having regard to its network architecture and the state of available technology.

8. Technical Measures may be implemented using each Licensee's existing systems and operational capabilities. The specific method or methods adopted by a Licensee under clause 5 may vary according to that Licensee's network architecture and technical circumstances, provided the outcome required by clause 5 is achieved.

9. **No Obligation to Assess or Re-Verify CSEAM**

For the avoidance of doubt, a Licensee is not required to access, view, assess or independently determine whether any online resource identified in Reference Data constitutes CSEAM, or to validate the accuracy of the Reference Data. The responsibility of a Licensee under this Determination is limited to implementing, in good faith, the applicable Technical Measures against Reference Data received through the authorised process set out in Part 3. Neither the Authority nor any Licensee is required to re-verify the underlying content of the Reference Data, which has been classified and supplied in accordance with the established procedures of the Authorised Source. The determination of what constitutes CSEAM rests exclusively with the relevant law enforcement agency; a Licensee acts solely, and in good faith, on the Reference Data as supplied to it.

Part 3 – Reference Data and Blocklist Governance

10. Responsibility for sourcing, validating, maintaining, auditing and reviewing the Reference Data rests with the Authorised Source, and not with any Licensee or the Authority.

11. The Authority will coordinate with the Authorised Source to facilitate, where necessary and to the best of its abilities, Licensees' receipt of Reference Data in accordance with the IWOL Agreement or such other arrangement as the Authorised Source may establish, whether by direct access to a system maintained by the Authorised Source or INTERPOL, by transmission of Reference Data from the Authorised Source, or by such other secure means as the Authorised Source may specify from time to time, in a format and at an update frequency settled through WG3 consultation.

12. Reference Data Updates

(a) Reference Data shall be updated from time to time as resources are added, amended or removed by the Authorised Source.

(b) Every Licensee must implement every Update within the applicable timeframe in paragraph (c). This applies equally to additions and to removals: a Licensee must cease restricting a resource that has been removed from the Reference Data within the same timeframe as applies to restricting a resource that has been added.

(c) The applicable timeframe, running from receipt of the Update by the Licensee through the agreed channel, is:

i. where the Licensee's systems receive and apply Updates automatically, upon receipt and without human intervention; and

ii. where paragraph (g) applies, the period specified in the Service Level Agreement approved by the Authority under that paragraph or, until such a Service Level Agreement is approved, at least once in every period of seven (7) days, where a list of Updates is available for application.

(d) Notwithstanding paragraph (c)(ii), where an emergency has been declared by the National Disaster Risk Management Office or the Government of Fiji and a Licensee's major time and effort is reasonably anticipated to be spent on assessing, strengthening or restoring its network as a result of that emergency, the Licensee may, by written notice to the Authority, apply Updates under paragraph (c)(ii) at least once in every period of [fourteen (14)] days instead of the period specified in that paragraph. That relaxation:

i. commences on the date of the Licensee's notice, which must identify the emergency and the anticipated impact on the Licensee's network and operations;

ii. ends on the date on which the emergency status is removed, upon which the Licensee must resume the timeframe in paragraph (c)(ii) and apply all outstanding Updates within [two (2) business days]; and

iii. may be extended by the Authority, on written application by the Licensee setting out the extent of the impact of the emergency on its network and operations, for such further period and on such terms as the Authority considers appropriate.

(e) Notwithstanding paragraph (c), a Licensee may, in its own judgement, implement a period during which it restricts any change to its network configuration other than emergency repair of network outages (a "Network Embargo") and in connection with significant national events. Where the Licensee has formally notified the Authority in writing of the start and end dates of a Network Embargo, the Licensee is not required to apply any Update during the Network Embargo and the timeframe in paragraph (c) does not apply to it. A Licensee must apply all outstanding Updates within [two (2) business days] after the notified end date, and must not extend a Network Embargo beyond that date without giving the Authority further written notice.

(f) As far as is practically possible, Updates shall be communicated to Licensees in a manner that enables Technical Measures to be applied proactively and automatically within Licensees' networks without human intervention, as and when Updates are received.

(g) Where a Licensee's technical, resource or system constraints preclude automatic Updates, WG3 shall, following consultation with Licensees and having regard to the update mechanisms of the Authorised Source, consider, develop and recommend Service Level Agreements to the Authority for the timely manual application of Updates, covering both additions and removals. The Authority may consider the same, reserving the right to require amendments and further consultation with the Licensees.

(h) A Licensee must record the receipt and implementation of each Update in the audit log required by clause 19.

13. A Licensee that implements Technical Measures in good faith in reliance on the then-current Reference Data supplied through the agreed channel, and that applies each Update within the applicable timeframe under clause 12, is taken to have complied with clause 5 in respect of that data, without prejudice to the protection available to the Licensee under Section 73(3) of the Act. A Licensee is not in breach of clause 5 or clause 12 by reason only of any delay between the making of an Update by the Authorised Source and its receipt by the Licensee.

Part 4 – Governance

14. Implementation coordination

Implementation coordination under this Determination shall be undertaken through WG3, the existing Industry and Technology Response working group established under the National Taskforce. WG3 shall serve the following functions under this Determination:

(a) settling the arrangements, data format and update frequency for the receipt of Reference Data and Updates in accordance with clause 11;

(b) considering, developing and recommending Service Level Agreements to the Authority for the manual application of Updates (additions and removals) where automatic update is not possible, in accordance with clause 12;

(c) reviewing and recommending on Licensee requests for extensions of time under clause 17; and

(d) addressing any other operational or technical matters necessary to give practical effect to this Determination.

15. WG3 does not exercise the regulatory powers of the Authority and has no authority to determine whether any content constitutes CSEAM, to alter the obligations imposed by this Determination, or to bind the Authority on any matter reserved to it under the Act.

Part 5 – Implementation

16. Phased Implementation

Licensees must implement Technical Measures in accordance with the following structure, which the Authority considers to be a reasonable and materially shortened timeframe, having regard to the fact that comparable Licensees already operate equivalent measures in other jurisdictions and that the Reference Data is sourced from a verified law-enforcement source rather than a vendor-compiled list, unless an alternative timeframe is approved by the Authority having regard to a Licensee's technical circumstances:

(a) Phase 1 – Establishment:

i. each Licensee shall execute the IWOL Agreement within 3 business days of receiving the same from either the Fiji Police Force or the Authority (whichever is earlier) provided that the Office of the Solicitor-General (Fiji) has reviewed and approved the execution of the same;

ii. each Licensee shall within a further 5 business days of executing the said IWOL Agreement, take such steps as are reasonably required to receive Reference Data in accordance with the arrangements established under, or pursuant to, the IWOL Agreement, whether by direct access to a system maintained by the Authorised Source or INTERPOL, by encrypted transmission of Reference Data from the Authorised Source, or by such other secure means as the Authorised Source may specify. This Determination comes into force under clause 2 regardless of when the IWOL Agreement is executed; however, no Technical Measures are required to be operationally applied under this Determination until Phase 1 is complete. Phase 1 is a precondition to Phase 2; and

(b) Phase 2 – Full Technical Implementation (as soon as practicable, and in any event no later than 7 business days after completion of Phase 1): each Licensee shall complete technical testing and deploy Technical Measures across its network, deploy the Landing Page in accordance with clause 28 (where technically supported), and commence ongoing monitoring and reporting in accordance with Part 6.

17. A Licensee may apply to the Authority for an extension of time to any phase in clause 16, supported by written reasons. WG3 may recommend that the Authority grant an extension.

Part 6 – Reporting and Audit

18. Reporting

(a) Each Licensee must provide quarterly compliance reports to the Authority, in a form agreed through WG3 consultation and consistent with the quarterly reporting cycle applicable to other regulatory obligations, addressing at minimum:

i. system availability;
ii. volume of Technical Measures applied;
iii. number and category of access restriction events; and
iv. material exceptions, technical incidents or service disruptions, including any Implementation Error and any failure to implement an Update within the applicable timeframe under clause 12.

(b) The first quarterly report shall be due three months after completion of Phase 2 under clause 16(b), or on such other date as the Authority may notify.

(c) A report must not contain the identity of any online resource comprised in the Reference Data, or any personal information identifying a user, consistent with clause 22.

19. Each Licensee must maintain an audit log of changes to its implementation of the Reference Data, which must record:

(a) for each Update:

i. the identity of the officer who received the Update and of the officer who implemented it;
ii. the time stamp (date and time) of receipt and of implementation;
iii. the filename of the Reference Data file received and applied; and
iv. the implementation status, being whether the Update was successfully implemented or not.

(b) for each Implementation Error, the same particulars as in paragraph (a) (including whether the Implementation Error was corrected), together with the dates of identification and of correction.

The audit log must refer to Reference Data by filename only and must not reproduce, list or otherwise record the content of the Reference Data, including any online resource comprised in it, consistent with clause 22. The audit log is to be made available to the Authority on request.

Part 7 – Data Governance and Privacy

20. Reference Data, and any records generated in the course of implementing this Determination, must be received, stored, accessed, retained and destroyed in accordance with arrangements settled through WG3 consultation, any applicable requirements of the IWOL Agreement, and applicable Fijian privacy and data protection law, including any National Privacy and Personal Data Protection Policy endorsed by Cabinet.

21. While Reference Data is within a Licensee's custody or control, the Licensee must:

(a) retain Reference Data for as long as is necessary for the implementation of the restrictions required under this Determination;

(b) maintain appropriate confidentiality, security and access controls over the Reference Data, including by restricting access to authorised personnel only;

(c) maintain records of access to Reference Data within its systems; and

(d) implement appropriate cybersecurity safeguards commensurate with the sensitivity of the Reference Data.

22. For operational security reasons, the specific online resources or domains comprised in the Reference Data, and any list of resources restricted under this Determination, must not be published or otherwise disclosed by the Authority, the Authorised Source, or any Licensee.

Part 8 – Errors, Dispute Resolution and Correction

23. Reference Data Errors and Implementation Errors

This Part distinguishes between errors in the underlying Reference Data and technical implementation errors by a Licensee. They are dealt with differently, as follows:

(a) **Reference Data Errors -** A complaint, report or concern that a legitimate online resource has been incorrectly included in the Reference Data must be referred by the Licensee, promptly, to the Fiji Police Force, for review and referral to the Authorised Source. A Licensee must not itself determine whether a resource has been correctly included in the Reference Data, consistent with clause 9, and must maintain the restriction until the resource is removed by an Update or the Licensee is directed in writing under clause 24(c).

(b) **Implementation Errors -** An Implementation Error is the responsibility of the Licensee concerned. A Licensee that becomes aware of an Implementation Error, whether through a complaint, its own monitoring or notice from the Authority, must promptly correct it, and in any event within [two (2) business days] of becoming aware or such other period as the Authority may allow; must notify the Authority of the error and its correction; and must record both in the audit log under clause 19. The Authority may direct a Licensee to correct an Implementation Error. A correction under this paragraph does not require a direction under clause 24.

(c) **Initial Check -** On receiving a complaint or report of an erroneous restriction, a Licensee must first check whether the restriction results from an Implementation Error (including a restriction extending beyond the resources identified in the Reference Data, or a failure to apply a removal), without assessing whether the resource constitutes CSEAM. If it does, paragraph (b) applies. If it does not, paragraph (a) applies. If the Licensee is unable to determine the cause, it must refer the matter under paragraph (a) and inform the Authority that an Implementation Error has not been excluded.

24. A Licensee must not remove or alter a restriction implemented under this Determination except:

(a) by applying an Update under clause 12, including a removal;
(b) to correct an Implementation Error under clause 23(b);
(c) upon written direction from the Authority or the Authorised Source; or
(d) as provided in clause 25.

25. Temporary Suspension

(a) The Authority may, on the application of a Licensee or on its own motion, direct a Licensee to temporarily suspend, modify or apply an alternative implementation of a Technical Measure where reasonably necessary to address:

i. material network disruption;
ii. erroneous implementation of a technical restriction;
iii. a cybersecurity risk affecting the Licensee's network or systems; or
iv. significant unintended restriction of lawful services.

(b) Any temporary suspension under this clause must be promptly notified to the Authority and is subject to ratification by the Authority. The Licensee must reinstate the relevant Technical Measure promptly upon direction from the Authority following resolution of the circumstances giving rise to the suspension.

(c) For the avoidance of doubt, the relaxation under clause 12(d) and a Network Embargo under clause 12(e) operate as extensions of the timeframe for applying Updates under clause 12. They are not a suspension, modification or alternative implementation of a Technical Measure for the purposes of this clause and do not require a direction or ratification by the Authority.

26. The Authority, in collaboration with the Authorised Source, will use its best endeavors to resolve correction or delisting requests referred under clause 23(a) within 7 business days of receipt.

Part 9 – Customer Notification

27. Each Licensee shall update its terms of service, to the extent required, to reflect measures taken in compliance with a lawful direction or determination of the Authority. Such updates must be completed within 1 month of the commencement of this

Determination, or such extended period as the Authority may allow having regard to the Licensee's circumstances.

28. Landing Page

(a) Where technically supported, a Licensee must redirect a user attempting to access an online resource restricted pursuant to this Determination to a Landing Page, rather than displaying an unexplained error or block message.

(b) The Landing Page must display, at a minimum, the content set out in Schedule 2, in plain language and legible on both mobile and desktop devices. That content must be provided in English and in such other languages as the Authority may approve.

(c) A Licensee may add its own branding, customer care contact details and additional language versions, but must not omit, alter or contradict the minimum content in Schedule 2 without the prior written approval of the Authority.

(d) The Landing Page must not list or otherwise disclose any other online resource comprised in the Reference Data, or display any personal information about the user, consistent with clause 22.

(e) Nothing in this clause requires a Licensee to decrypt, intercept or inspect encrypted communications in order to display the Landing Page. Where redirection to the Landing Page is not technically supported, the Licensee remains subject to clause 5 and must, where practicable, display a notice containing the content in Schedule 2 or as much of it as is technically possible.

(f) A report of an erroneous restriction made through a Licensee's customer care channels, as contemplated by Schedule 2, must be handled by the Licensee in accordance with Part 8.

(g) The Authority may, after consultation with the Fiji Police Force and, through WG3, other relevant stakeholders, amend Schedule 2 (including support service contact details) by written notice to Licensees. Licensees must give effect to the amendment within the reasonable period specified in the notice.

29. Public Communication

(a) Public communication regarding the existence, nature and legal basis of the measures under this Determination shall be coordinated by the Authority and the Fiji Police Force as lead agencies. Such communication may include:

i. publication of a public notice in a newspaper of general circulation in Fiji;
ii. communication through official government and Authority digital and social media channels; and
iii. amplification by Licensees through their own customer communication channels.

(b) Licensees are authorised to refer customers to the public notice issued by the Authority and the Fiji Police Force for information about the measures in place.

30. Individual customer notification is not required except in accordance with guidance issued by the Authority, and must not disclose sensitive information or create a secondary risk to any person.

Part 10 – Protection from Liability

31. Nothing in this Determination limits or affects any protection available to a Licensee under Section 73(3) of the Act or the Authority under Section 72(3) of the Act.

32. **Good Faith**

(a) Without limiting clause 31, a Licensee that implements a Technical Measure in good faith in reliance on Reference Data supplied in accordance with this Determination (including an Update) does not thereby incur civil liability to any person in respect of the implementation of that Technical Measure, including where the Reference Data is later found to contain a Reference Data Error.

(b) Paragraph (a) does not apply to the extent that a restriction results from an Implementation Error. Nothing in this paragraph limits the protection available to a Licensee under Section 73(3) of the Act.

Part 11 – Costs

33. This Determination does not establish a cost-recovery mechanism. The Authority may consider matters relating to the cost of implementation and make recommendations through WG3 consultation with Licensees.

Part 12 – Review

34. The Authority may review this Determination at any time, and will in any event review it no later than 12 months after its commencement, having regard to any recommendations of WG3 and Licensees.

Part 13 – General

35. Written reasons for this Determination, including the Authority's consideration under Section 21 of the Act, are set out at Schedule 1, in accordance with Sections 18(3)(c) and 22(e) of the Act.

36. This Determination takes effect from the date specified in clause 2.

37. **Non-compliance, Enforcement and Penalties**

(a) The obligations imposed by this Determination are binding on each Licensee. This Determination does not itself prescribe penalties; the consequences of non-compliance are those provided by the Act.

(b) Without limiting any other power of the Authority, non-compliance by a Licensee with any obligation under this Determination may be addressed by the Authority under the Act, including under:

i. section 76 (contraventions and breaches);
ii. section 77 (notice to show cause, and the imposition of directions and penalties and the variation, suspension or revocation of a licence);
iii. section 78(1)(c) (written direction to undertake or cease a specific action);
iv. section 79 (desist orders, following a determination under section 18 that a determination has been violated); and
v. sections 17 and 31 (monitoring, investigation and the power to require information, including the audit log and records under clause 19).

(c) Where possible non-compliance by a Licensee comes to light in the course of a criminal investigation, or is otherwise identified by the Fiji Police Force or another law-enforcement agency, the Authority may receive that information and take action under paragraph (b). A Licensee must give such help to officers and authorities of the Government as is required by Section 73(2) of the Act, and the Authority may disclose information about a Licensee's compliance to such agencies where permitted by the Act, including Section 30(4).

(d) In deciding what action to take under paragraph (b), the Authority will have regard to whether the Licensee acted in good faith, applied each Update within the applicable timeframe, promptly corrected any Implementation Error, and used reasonable efforts as contemplated by clauses 7 and 8, and to any extension granted under clause 17 or suspension directed under clause 25.

38. In the event of any inconsistency between this Determination and the IWOL Agreement, or any other agreement or arrangement between a Licensee, the Authorised Source, or INTERPOL for the receipt of Reference Data, this Determination prevails to the extent of the inconsistency, except to the extent that compliance with this Determination would place a Licensee in breach of a mandatory requirement of that agreement, in which case the Authority will consult with the Licensee and the Authorised Source with a view to resolving the inconsistency.

Issued by: **Telecommunications Authority of Fiji**

Chairperson

Date: 05 | 11 | 2026

TELECOMMUNICATIONS AUTHORITY OF FIJI
THE COMMON SEAL OF

Schedule 1 – Written Reasons

(Sections 18(3)(c) and 22(e) of the Act)

1. The Authority issued a Notice of Proposed Determination on 6 August 2026, inviting submissions from all Licensees providing an Internet Access Service on the matters set out at paragraphs (a)–(i) of the Notice.

2. The Authority received written submissions from three Licensees providing an Internet Access Service, from 17 August to 25 September 2026. Each submission was considered by the Authority on its merits, and the measures adopted in this Determination apply uniformly to all Licensees.

3. Having regard to those submissions, the Authority has:

   (a) confirmed that responsibility for sourcing and maintaining the Reference Data rests with the Authorised Source, consistent with the position of the responding Licensees;

   (b) adopted a phased implementation timeframe, materially shortened from that proposed in the submissions and tied to execution of the INTERPOL Worst-of List data-sharing agreement rather than to the date of this Determination, noting that Licensees were given advance notice of the Authority's intended engagement with the IWOL programme on 12 June 2026, for the reasons set out at paragraph 3(g) below;

   (c) confirmed the application of Section 73(3) protection, and an express statement that no civil liability arises from good-faith reliance on Reference Data, addressing the liability concerns raised in the submissions received;

   (d) acknowledged the technical limitations of Licensees in respect of encrypted traffic, VPNs, Tor and content delivery networks, addressing the matter raised in the submissions received;

   (e) confirmed that no Licensee is required to access, view, assess or independently determine whether content constitutes CSEAM, or to re-verify the Reference Data, addressing the matter raised in the submissions received;

   (f) confirmed that implementation coordination shall be undertaken through WG3, the existing industry and technology working group established under the National Taskforce, rather than through a separate governance body;

   (g) determined that the implementation timeframe proposed in submissions should be materially shortened, having regard to the fact that comparable Licensees already operate equivalent measures in other jurisdictions and that the Reference Data is sourced from a verified law-enforcement source rather than a vendor-compiled list, noting that the precise technical means by which Reference Data will be made available to Licensees has not yet been finalised, and that a Licensee may apply under clause 17 for an extension of time where genuinely necessary;

(h) confirmed that non-compliance with this Determination may be addressed through the enforcement powers of the Authority under the Act, as set out in clause 37, in addition to the specific measures provided for in this Determination;

(i) adopted measures to support affected users, including requiring Licensees, where technically supported, to redirect users to a Landing Page rather than an unexplained block notice, while ensuring that the Reference Data and any list of restricted resources are not publicly disclosed, for operational security reasons;

(j) noted that any Licensee aggrieved by this Determination may lodge an appeal pursuant to section 66 of the Telecommunications Act 2008;

(k) adopted reporting and audit requirements in Part 6, applicable to every Licensee, for the reasons set out at paragraph 5 below;

(l) provided that Updates to the Reference Data comprise both additions and removals, having regard to confirmation received from INTERPOL that updates to the IWOL include both, and required every Licensee to implement both within the applicable timeframe in clause 12, so that restrictions remain current and a resource removed from the Reference Data is not restricted for longer than necessary;

(m) prescribed at Schedule 2 the minimum content of the Landing Page, so that every user is given the same clear explanation of why access has been restricted, that CSEAM causes real harm to children and survivors, that such material is illegal in Fiji, where support is available, and how to report a suspected erroneous restriction, rather than leaving that content to individual Licensees; and

(n) distinguished, in Part 8, between Reference Data Errors, which are referred to the Authorised Source for review, and Implementation Errors, which the Licensee concerned must promptly correct, because the responsibility for correcting each lies with a different party.

4. Consideration of Regulatory Burden — Section 21

In accordance with section 21 of the Act, the Authority has considered the effect of this Determination on both users and Licensees, and whether the reasonably anticipated benefits to users outweigh the regulatory burden reasonably anticipated to be placed on Licensees.

Benefits

The reasonably anticipated benefits of this Determination include:

(a) reducing access through Fiji's telecommunications networks to material associated with the serious criminal victimisation of children, thereby directly reducing harm to some of the most vulnerable members of society;

(b) protecting children and users of Fiji's telecommunications networks from exposure to CSEAM;

(c) reducing the use of Fiji's telecommunications infrastructure in connection with offences under section 62A of the Juveniles Act 1973 and any related provision;

(d) supporting the discharge by the Authority and Licensees of their respective statutory obligations under sections 72 and 73 of the Act; and

(e) reflecting INTERPOL's own recognition that access blocking of this kind is a preventive, transparent and informative measure, benefiting the public by preventing further victimisation of children, shielding internet users from unintentional exposure to harmful material, and preventing access by those seeking such material (see INTERPOL, "Blocking and Categorizing Content").

Burden

The Authority recognises that implementation may require Licensees to:

(a) execute the IWOL Agreement and put in place the arrangements necessary to receive Reference Data;

(b) undertake technical configuration, system testing and deployment before full implementation;

(c) maintain appropriate records, audit logs and access controls over Reference Data;

(d) provide quarterly compliance reports and participate in WG3 consultation processes;

(e) incur associated implementation and operational costs, including costs relating to system configuration, staff training, security controls, ongoing list updates, compliance reporting and complaints handling;

(f) manage operational risks arising from their differing network architectures, including the potential for over-blocking of legitimate content;

(g) comply with a compressed implementation timeframe, reflecting the Authority's assessment that a shorter period than that proposed in submissions is justified having regard to Licensees' existing operational capabilities and the verified nature of the Reference Data, and having regard to the advance notice given to Licensees on 12 June 2026;

(h) implement both additions and removals of Reference Data within the applicable timeframe, and record them in the audit log;

(i) display the Landing Page with the minimum content prescribed in Schedule 2, where technically supported; and

(j) promptly correct any Implementation Error and notify the Authority.

In assessing that burden, the Authority has taken into account the submissions received from Licensees concerning technical capability, implementation timeframes, operational impacts and costs.

Mitigations

The Authority has sought to minimise the regulatory burden by:

(a) requiring only reasonable and proportionate Technical Measures using each Licensee's existing systems and capabilities;

(b) not requiring the decryption or inspection of encrypted communications;

(c) using externally verified Reference Data, sourced and validated exclusively by the Authorised Source rather than by Licensees or the Authority;

(d) confirming that no Licensee is required to independently assess whether content constitutes CSEAM or to re-verify the Reference Data, thereby removing the most operationally burdensome aspect of alternative approaches;

(e) adopting a phased implementation approach that allows Licensees to progress through testing and rollout in a structured and technically manageable sequence;

(f) providing for temporary suspension of Technical Measures where reasonably necessary to address material network disruption, erroneous implementation, cybersecurity risk or significant unintended over-blocking;

(g) coordinating implementation through the existing WG3 framework, avoiding the burden of establishing a separate governance structure;

(h) confirming that a Licensee incurs no civil liability for implementing a Technical Measure in good faith reliance on Reference Data;

(i) providing a defined extension mechanism, and by keeping the specific contents of the Reference Data confidential to reduce operational security risk;

(j) the advance notice given to Licensees on 12 June 2026 regarding the Authority's intended engagement with the IWOL programme, affording Licensees an extended period to prepare in advance of this Determination;

(k) prescribing standard minimum Landing Page content, so that Licensees need not develop that content themselves, and not requiring redirection where it is not technically supported; and

(l) keeping Reference Data Errors with the Authorised Source, so that Licensees are not required to resolve them.

Conclusion

Having regard to the nature and seriousness of the harm addressed by this Determination, the targeted scope of the proposed measures, the safeguards incorporated into the Determination and the implementation flexibility afforded to Licensees, the Authority considers that the reasonably anticipated benefits to users outweigh the regulatory burden reasonably anticipated to be placed on Licensees.

5. **Reasons for the Reporting and Audit Requirements (Part 6)**

The reporting and audit requirements in Part 6 apply uniformly to every Licensee providing an Internet Access Service, irrespective of the Licensee's size, ownership, technology or network architecture, and have not been framed by reference to any individual Licensee. The Authority considers them necessary and proportionate for the following reasons:

(a) the Determination imposes an outcome-based obligation under clause 8, and the method adopted may differ between Licensees. Reporting is the means by which the Authority can verify, consistently across different network architectures, that the required outcome is being achieved, and so discharge its own obligation under section 72(1) of the Act;

(b) reporting allows the Authority to identify and respond promptly to over-blocking, technical incidents, service disruptions and Implementation Errors, including by exercising its powers under clause 25;

(c) the information reported will inform the review of this Determination under clause 34 and the recommendations of WG3;

(d) the minimum content of each report is limited to aggregated operational information (system availability, volume of Technical Measures applied, the number and category of access restriction events, and material exceptions), and must not disclose the resources comprised in the Reference Data or any personal information about users, consistent with clause 22;

(e) the form of the reports is to be agreed through WG3 consultation with Licensees, and the quarterly cycle is consistent with the reporting cycle applicable to other regulatory obligations, with the first report due only three months after completion of Phase 2, so as to minimise the burden on Licensees; and

(f) the audit log required by clause 19 records information that a Licensee must in any event hold in order to implement the Reference Data, is made available only on request, and enables the Authority to verify that both additions and removals are implemented within the applicable timeframe.

6. The Authority considers that this Determination is necessary to further the objectives of Section 3 of the Act and to give practical effect to the best-endeavors obligations in Sections 72 and 73 of the Act.

Schedule 2 – Minimum Content of the Landing Page
(Clause 28)

The Landing Page must display, at a minimum, the following content: (text in capitals is a heading)

ACCESS TO THIS WEBSITE HAS BEEN RESTRICTED

Access to this website has been restricted in accordance with a Determination issued by the Telecommunications Authority of Fiji under the Telecommunications Act 2008. The website has been identified by law enforcement, through an internationally recognised child protection mechanism, as containing child sexual exploitation and abuse material (CSEAM).

Child sexual exploitation and abuse causes serious and lasting harm to children and survivors. Such material is illegal in Fiji. Accessing, viewing, possessing, producing or distributing it may constitute a criminal offence under Fiji law, including section 62A of the Juveniles Act 1973.

HELP IS AVAILABLE

If you are a child experiencing abuse, are concerned about a child's safety, or need confidential support or counselling, assistance is available through:

- *Child Helpline Fiji – 1325 (toll-free)*
- *Lifeline Fiji – 1543 (toll-free)*

THINK THIS RESTRICTION IS A MISTAKE?

If you believe this website has been restricted in error, you may report the matter through your Internet Service Provider's customer care channels for review.

-END-