ilma

Foundation

Child Online Safety in Mauritius: A Rights-Based and Comprehensive Protection Framework

Protecting children online is not only an obligation — it is an investment in the very future of Mauritius

Prepared for: Ministry of Information Technology, Communication and Innovation (MITCI), Republic of Mauritius

Prepared by: ILMA Foundation

✉ contact@ilmafoundation.com

☎ +230 5251 5351

http://www.ilmafoundation.com

CONTENTS

PREAMBLE

This report has been prepared by ILMA Foundation in direct response to the public consultation initiated by the Ministry of Information Technology, Communication and Innovation (MITCI) on the Draft Child Online Safety Policy for Mauritius.

The advent of digital technologies has fundamentally reshaped the environment in which children grow, learn, and interact. While the internet offers immense educational, social, and developmental opportunities, it simultaneously exposes minors to a spectrum of online risks, including exploitation, harmful content, and breaches of privacy. In this context, the safeguarding of children online emerges not only as a national priority but also as an international human rights obligation.

In addressing these challenges, it is essential that child protection measures are carefully calibrated to preserve fundamental rights, including freedom of expression, the right to access information, the right to privacy, and parental authority. An effective child online safety framework must strike an appropriate balance: ensuring that children are shielded from online harms without enabling unwarranted restrictions, censorship, or disproportionate control over digital spaces.

This submission is founded upon three guiding principles:

1. The paramountcy of the best interests of the child, in accordance with the United Nations Convention on the Rights of the Child (CRC) and regional standards.
2. The necessity for any restrictions or interventions to comply with the principles of legality, necessity, proportionality, and legitimate aim, as articulated in international human rights law.
3. The imperative of fostering an ecosystem of shared responsibility, where government, parents, educators, industry, and civil society actors collectively contribute to a safe, empowering, and rights-respecting digital environment.

Drawing upon comparative international frameworks, empirical research, and the socio-legal context of Mauritius, this report aims to complement and strengthen the policy development process. It offers a series of recommendations and observations with particular emphasis on ensuring that protective mechanisms are not inadvertently instrumentalized for purposes of unjustified content control or political censorship.

ILMA Foundation commends the Ministry for its inclusive and consultative approach. We trust that this submission will assist in the elaboration of a comprehensive, future-proof, and rights-compatible framework for the protection of children online in Mauritius.

CONTRIBUTORS

ME. Assadullah **DURBARRY**

Assadullah operates at the intersection of law, technology, and education—designing systems and sharing knowledge that empower individuals and institutions to thrive in a fast-evolving world. With experience leading automation and data initiatives at Cisco, and legal qualifications in both Mauritius and Australia, I bring a unique blend of operational, legal, and academic insight. Through my work as a lecturer, legal professional, and founder of the ILMA Foundation, I am committed to advancing education, promoting ethical innovation, and driving sustainable development rooted in justice and human rights.

Mr. Umar **MAWLAH**

Umar has been an educator at Port Louis High School since 2010, following valuable teaching experience at Doha Secondary School in 2009. He holds a Bachelor of Science in Biology from the University of Mauritius and a Diploma in Multimedia. Umar later pursued a Postgraduate Certificate in Education (Science with Biology) and a Postgraduate Diploma in Education, while also earning a Certificate in Interior Design. Passionate about continuous learning and research, Umar blends science, technology, and creativity in his teaching. With over a decade of experience, he inspires students through innovative and research-driven approaches to education.

ME. Mehdi **JAUNBOCUS**

Mehdi Jaunbocus is a dual-qualified Barrister-at-Law admitted in both England and Wales and Mauritius, with a well-rounded legal practice spanning civil litigation, advisory work, and transactional matters. With experience across reputable chambers including Goburdhun Chambers, Matrix Legal, and LexTech Chambers, Mehdi has developed a strong command of litigation strategy, contract drafting, and risk management. Known for his analytical precision and client-centric approach, he consistently delivers effective legal solutions grounded in integrity and professional excellence. Mehdi's international training and academic background further enhance his ability to navigate complex legal challenges with clarity and strategic insight.

ME. Bibi Nafiisah **JEEHOO**

Nafiisah is a Senior Associate in the Mauritius office of Bowmans where she advises in investment funds, corporate, tax and commercial law matters. Prior to joining Bowmans Mauritius, she was a member of the financial services and capital markets team of a leading law firm in Mauritius where she was involved mainly in the formation of private equity funds, private equity transactions, securities offerings and listing of entities. She has read law at the University of Mauritius and completed the Bar Professional Training Course at Northumbria University. She is also an Affiliate of the Association of Chartered Certified Accountants (ACCA). She was called to the Bar of England & Wales in 2014 at the Honourable society of Lincoln's Inn.

ABSTRACT

The digital revolution has transformed children's lives in Mauritius, offering unprecedented opportunities for education, communication, and personal development. However, the rapid expansion of internet access has simultaneously exposed minors to serious online risks, including cyberbullying, grooming, exploitation, harmful content, and data misuse.

While Mauritius has taken preliminary steps through initiatives such as the Cybersecurity and Cybercrime Act 2021 and MAUCORS+, there remains a critical gap: the absence of a dedicated, child-specific, and rights-compliant framework to safeguard children in the digital environment.

In response to the Ministry of Information Technology, Communication and Innovation's public consultation, this report proposes a comprehensive, structured, and principled Child Online Safety Framework that balances the need for robust child protection with the imperative to uphold fundamental freedoms — notably, freedom of expression, access to information, and privacy.

Drawing from international best practices (Singapore, UAE, Scandinavia, Malaysia, China), and aligned with global rights frameworks (CRC, ICCPR), the key recommendations of this submission include:

- **Establishing a Digital Age of Consent (18–20 years)**, requiring verified parental consent for minors to engage online.
- **Mandatory Age Verification Mechanisms** for all platforms operating in Mauritius.
- **Strengthening Legal Frameworks** to criminalize emerging online offenses such as grooming, sextortion, and live-streamed exploitation.
- **Restricting Social Media Access by Age Tier**, with a complete ban under 14 and graduated supervision between 14–18.
- **Implementing Data Collection and Profiling Safeguards** for minors, including mandatory data purges at the age of majority.
- **Mandating Content Filtering by Age Group**, following a model similar to Douyin (China's version of TikTok), focusing on educational and motivational content for minors.
- **Enforcing Online Gaming and Gambling Regulations**, including mandatory age checks and time restrictions for minors.
- **Creating Child-Only Digital Spaces** to limit exposure to adult users and interactions.

Institutional innovations proposed include the establishment of a Child Online Protection Ombudsman (COPA) with independent authority to issue binding takedown orders, manage a child-specific incident reporting system, and liaise with international child safety networks.

In parallel, the report underscores the necessity of empowering parents and educators through national digital literacy programs, the creation of a Digital Parenting Portal, community engagement campaigns, and integration of digital resilience education into school curricula from an early age.

The proposed strategy is phased across three years, combining immediate legislative actions, medium-term capacity-building, and long-term evaluation through a dynamic, evidence-based monitoring framework. Key milestones include the enactment of a Child Online Protection Act, the operationalization of COPA, and the publication of annual Child Online Safety Reports to Parliament. The expected outcomes extend beyond protecting children:

- Strengthened family and educational environments;
- Safer digital ecosystems;
- Enhanced national and international reputation as a child-friendly, rights-respecting digital society;
- And the fostering of a digitally resilient generation.

This submission emphasizes that child online safety must not be pursued at the cost of democracy. Measures must be lawful, necessary, proportionate, transparent, and subject to independent oversight to prevent the misuse of content moderation structures for political or improper purposes.

The ILMA Foundation remains committed to assisting policymakers, educators, industry stakeholders, and the Mauritian public in building a digital environment where every child can explore, learn, and thrive — safely, confidently, and freely.

ilma

Foundation

Comprehensive Policy Report

CONTENTS

1.0 INTRODUCTION

The digital age has transformed the way children grow, learn, and interact. Across the world, access to the internet and online services has become not just a luxury, but a core component of education, communication, and social development. Mauritius, as a nation committed to technological progress, is no exception.

While the internet offers unprecedented opportunities for learning and exploration, it also exposes children to a range of threats. The vulnerabilities of minors online — from cyberbullying to exposure to harmful content, from grooming by predators to exploitation through online games and gambling mechanisms — are no longer theoretical. They are pressing, real-world concerns that require urgent, structured action.

Mauritius has already recognized the seriousness of these challenges, as reflected in the Cybersecurity and Cybercrime Act 2021 and initiatives like MAUCORS+. However, without a targeted child-specific framework, current measures risk being either too general or insufficiently protective. Worse, without appropriate safeguards, measures intended to protect children could inadvertently suppress free expression, intrude on privacy, and pave the way for broader censorship under the guise of child protection.

This report seeks to bridge the gap between necessary child protection and the preservation of digital rights. It proposes a new model for Mauritius — one that is proactive, rights-based, and tailored to the realities of the online world our children inhabit. It recognizes that protection must involve not just restrictions, but empowerment: equipping children, parents, and educators with the tools, knowledge, and structures they need to navigate the digital world safely.

The objective is to build an online environment in Mauritius where children are free to learn, explore, and thrive — safely, securely, and with their fundamental rights intact.

2.0 INTERNATIONAL PERSPECTIVES

A range of approaches exists globally, from Singapore's robust platform accountability to Scandinavia's education-first models. However, few models grapple deeply with the risk of governments misusing content filtering under the guise of child protection. These have been explained carefully in Appendix 1. Mauritius must learn from their successes but also innovate to uphold democratic principles.

Key lessons:

- Strict enforcement (Singapore)
- Comprehensive legal updating (Malaysia)
- Public education campaigns (UAE)
- Technological curfews and youth modes (China)
- Digital resilience education (Scandinavia)

3.0 THE CURRENT LANDSCAPE AND CHALLENGES IN MAURITIUS

Mauritius boasts one of the highest internet penetration rates in Africa, with nearly 64% of the population using the internet daily. Mobile device usage among children is also increasing rapidly, with smartphones, tablets, and gaming consoles becoming integral to their social and educational lives. Social media platforms such as Instagram, TikTok, WhatsApp, and YouTube dominate online interactions, even among pre-teens.

Yet with this growth has come exposure to substantial risks. Reports from local NGOs and MAUCORS+ indicate a rise in:

- Cyberbullying, especially among secondary school students;
- Grooming attempts, facilitated by anonymity and encrypted communications;
- Exposure to sexually explicit or violent content, often via international platforms without local moderation;
- Addiction to online gaming, including exposure to loot boxes, in-game purchases, and covert gambling mechanics;
- Privacy breaches, with children's personal data harvested for commercial profiling.

Existing laws — notably the Cybersecurity and Cybercrime Act 2021 and the Children's Act 2020 — provide a foundation but are fragmented and insufficiently child-focused. Critically, there is no standalone child online safety law that consolidates protection mechanisms, imposes direct obligations on tech companies, or enshrines a child-specific rights framework in Mauritius.

Moreover, enforcement remains weak. Many social media platforms do not have a physical or operational presence in Mauritius, making it difficult for regulatory bodies to enforce content removal or data protection orders. Furthermore, the current reliance on ISPs for voluntary filtering and takedown lacks consistency and is vulnerable to political manipulation.

Thus, while Mauritius has taken commendable first steps, it urgently requires a comprehensive, structured, and rights-respecting child online safety framework adapted to its local socio-legal context.

4.0 ETHICAL CONSIDERATIONS: FREEDOM OF EXPRESSION VS PROTECTION

As Mauritius moves to strengthen child online safety, it must tread carefully to avoid undermining two fundamental democratic values: freedom of expression and freedom of access to information. International human rights frameworks, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (to which Mauritius is a party), underscore that restrictions on speech must be lawful, necessary, and proportionate.

Child protection cannot be allowed to become a pretext for broad-based online censorship. The use of Internet Service Providers (ISPs), AI filtering systems, or third-party content moderators must be strictly limited to measures:

- That are clearly defined by law;
- Targeted specifically at harmful content (e.g., child pornography, grooming attempts, egregious cyberbullying);
- Subject to judicial oversight and due process mechanisms.

There is a tangible risk in the Mauritian context that content moderation structures, once created, could be misused to block dissenting voices, political criticism, or culturally sensitive but legitimate content. This risk is amplified in small island jurisdictions where political and regulatory bodies often operate in close proximity.

Thus, while this report advocates for stronger child protection, it categorically opposes any system that enables unchecked ISP-level censorship or blanket filtering of online content without transparent procedures and rights to challenge decisions.

Principles to be enshrined:

- Necessity: Only what is absolutely needed to protect children.
- Proportionality: Measures must not overreach into lawful speech.
- Transparency: Filtering systems and takedown processes must be publicly auditable.
- Independent Oversight: Establishment of a neutral body (such as a Child Online Ombudsman) to review takedown and content moderation actions.
- Appeal Mechanisms: Platforms and users must have the right to contest takedown orders.

Mauritius must build a system that empowers children and families, rather than one that disempowers society at large. Child protection must strengthen, not weaken, the foundation of a free, democratic digital space.

5.0 CORE RECOMMENDATIONS

Drawing on the best international practices and adapted to the Mauritian socio-legal context, the following core policy recommendations form the heart of the proposed Child Online Safety Framework.

5.1 Establish a Digital Age of Consent (18–20 years)

Mauritius should legislate a Digital Age of Consent at 18 years, aligning online data protection standards with the age of majority for marriage, contracts, and legal capacity.

- Children under 18 should require verified parental or guardian consent before being allowed to create accounts on online platforms that collect or process their personal data.

- For children aged 14–17, a graduated consent model should apply, whereby parents verify account creation and maintain oversight access.

- Below 14 years, the creation of any social media account or participation in open online platforms should be prohibited.

This model addresses the inconsistency between protecting minors in physical spaces but exposing them freely to online risks.

5.2 Enforce Mandatory Age Verification Mechanisms

All platforms accessible in Mauritius must be required to implement strong, privacy-protective age verification systems. This may include:

- ID-based verification (National ID or Passport).
- Verified payment methods (e.g., credit card check).
- Mobile phone verification tied to a responsible adult's number.

Platforms must be prohibited from relying solely on "self-declared" age fields without verification.

5.3 Strengthening Legal Frameworks Against Online Child Exploitation

Mauritius must update its legislative framework to explicitly criminalize modern online harms against children, including:

- Online grooming attempts.
- Sexual extortion ("sextortion").
- Possession and distribution of child sexual abuse materials (CSAM) over encrypted platforms.

Additionally, legislative reforms should impose mandatory reporting obligations on ISPs, digital platforms, and online service providers. Following models such as the UAE's Wadeema's Law, companies must be required to report suspected cases of child exploitation promptly to national authorities.

Safety by Design principles must be legally mandated — requiring default privacy settings for minors, age verification for access to adult content, and the disabling of algorithmic amplification of harmful content for users under 18.

Law enforcement bodies must also be strengthened. Specialized cybercrime units should be expanded and equipped with the technical capacity to investigate hidden networks, encrypted apps, and the dark web.

Procedures should be reformed to adopt victim-centric, trauma-informed practices, including child-sensitive interviewing protocols and access to psychological support for affected minors.

Finally, the government should systematically monitor legal enforcement effectiveness by:

- Tracking the number of online child exploitation investigations, prosecutions, and convictions annually;
- Measuring reporting rates from the public (to assess awareness and trust);
- Publishing annual transparency reports reviewing legal system performance.

5.4 Restrict Minor Access to Social Media Based on Age Tiers

- Under 14: No access to social media platforms. Strict ban.
- 14–16: Conditional access upon verified parental consent; periodic parental notifications if the child accesses sensitive content or usage spikes during "danger hours" (e.g., midnight to 6 a.m.).
- 16–18: Standard access, but mandatory opt-in for additional privacy and safety controls.
- 18+: Full adult access.

Social media companies must enforce these measures specifically for users located in Mauritius.

5.5 Data Collection, Storage, and Profiling Safeguards

Platforms must:

- Collect only essential data from minor users (minimalist data model).
- Prohibit profiling, targeted advertising, and data sales relating to minors.
- Purge all accumulated data once the minor reaches 18, unless express adult consent is obtained.
- Offer opt-in, not opt-out, for any additional data usage beyond the minimum necessary for account functionality.

5.6 Mandate Content Filtering by Age Group (Inspired by Douyin Model)

Platforms should automatically restrict the content available to minors, offering:

- Educational, motivational, and health-positive content feeds.
- Prohibition of sexually explicit, violent, gambling, or other harmful content streams.
- Regular parental reports showing category exposure for minors' accounts.

For example, TikTok's Chinese version, Douyin, only allows minors to see pre-approved educational and motivational videos during limited hours. Mauritius can adapt a similar, localized model.

5.7 Pornography and Online Gambling Restrictions

- All adult content platforms must implement strict age-verification gates that go beyond self-attestation.
- Mandatory credit card verification or government-approved age validation systems should be required.
- Platforms offering lootboxes, skins trading, or similar gambling-like mechanisms (e.g., Fortnite, CS:GO) must be regulated under gambling laws, requiring 18+ verification.

5.8 Regulate Gaming Time and Online Presence

- Minors under 14 should have access limited to a maximum of 90 minutes per day.
- Ages 14–17 should be capped at 4 hours/day.
- Mandatory offline hours enforced between 10 p.m. and 6 a.m..
- Special provisions can allow relaxed restrictions during public holidays and school vacations.

This is consistent with international best practices already deployed in countries like China and South Korea.

5.9 Introduce National 'Child-Only' Digital Spaces

Where feasible, encourage the development of child-safe online spaces and "walled gardens," where minors can interact only with verified other minors within their age group. Such ecosystems would reduce exposure to adult interactions and potential grooming threats.

6.0 INSTITUTIONAL MECHANISMS

To make any child online safety framework meaningful, Mauritius must establish strong and independent institutional structures capable of enforcing the laws, handling complaints, and providing swift remedies to children and parents. The following institutional measures are recommended:

6.1 Creation of a Child Online Protection Ombudsman (COPA)

A Child Online Protection Authority (COPA) should be established as an independent authority tasked with coordinating and enforcing all national efforts related to child online safety. COPA's functions should include:

- Receiving, investigating, and resolving complaints related to harmful online content, harassment, grooming, and other child-targeted digital abuses;
- Issuing mandatory takedown notices to platforms, ISPs, and hosting services regarding harmful content involving minors, with a 24-hour compliance deadline;
- Providing advisory opinions on the development, review, and updating of online safety policies and legislation;
- Overseeing parental complaint handling against platforms that fail to protect children properly;
- Publishing annual reports to Parliament to ensure transparency, accountability, and public trust.

Beyond handling complaints, COPA should be empowered to act as the national coordinating agency under the Ministry of Information Technology, Communication and Innovation (MITCI), continuously monitoring emerging digital threats and issuing binding compliance guidelines to industry actors.

It should also serve as Mauritius' official liaison to international initiatives such as the WePROTECT Global Alliance and the INHOPE network, ensuring that the country remains aligned with global best practices and benefits from international intelligence and cooperation on child online protection.

The Ombudsman's office must be adequately resourced, accessible to minors and their families, and capable of taking proactive leadership in creating a safer digital environment for all Mauritian children.

6.2 Establishment of a 24-Hour Mandatory Takedown Mechanism

Where harmful content involving minors (e.g., cyberbullying, grooming, sexual exploitation material) is identified:

- Platforms must comply with a takedown notice issued by COPA within 24 hours.
- Failure to comply should lead to graduated sanctions, including fines, content blocking, or operational restrictions in Mauritius.

A fast-tracked judicial review system must be available to platforms that wish to contest takedown orders, ensuring that free expression rights are preserved while prioritizing child protection.

6.3 Enhancing Child-Friendly Reporting and International Collaboration

While Mauritius' Cybercrime Online Reporting System (MAUCORS+) already allows the public to report cyber incidents, a dedicated child-friendly reporting interface must be developed to ensure accessibility for minors.

This simplified portal should:

- Use child-appropriate language and design;
- Offer clear categories for reporting issues like cyberbullying, grooming, and exposure to inappropriate content;
- Allow anonymous submissions while maintaining confidentiality protections.

All reports involving minors should be triaged rapidly, with serious cases (e.g., active grooming or exploitation threats) escalated to law enforcement within one hour where needed.

Mauritius should also formalize its engagement with global child protection networks by becoming a member of the INHOPE network (International Association of Internet Hotlines). Joining INHOPE would provide access to a worldwide database of CSAM reports, enhance the ability to request fast global takedowns, and ensure that Mauritius plays an active role in the international fight against online child exploitation.

By improving local reporting channels and strengthening international cooperation, Mauritius can ensure faster, more effective responses to child online harms while reinforcing its position as a serious digital safety jurisdiction.

6.4 Anonymous Reporting Systems

Mauritius should launch anonymous and confidential reporting channels, accessible via:

- Text messaging (SMS shortcode).
- Web forms.
- Mobile app-based reporting.

Reports should cover:

- Cyberbullying.
- Grooming attempts.
- Dissemination of unsolicited sexual imagery (e.g., "dick pics").
- Online gambling targeting minors.

Anonymous reporting reduces the fear of retaliation and can empower children, peers, parents, and teachers to intervene early before harm escalates.

All reports should be triaged by COPA and referred either for immediate action (e.g., takedown, police referral) or for supportive intervention (e.g., counseling, parental notification).

6.5 Publicly Available Blacklists and Accountability

The Ombudsman should maintain a publicly available blacklist (without exposing private information) showing:

- Platforms or sites consistently non-compliant with child protection standards.
- Statistics on types of complaints received and resolved.
- Progress reports on international cooperation to tackle cross-border abuses.

Transparency will help parents, educators, and minors make informed choices about the platforms they use, while pressuring companies to comply proactively.

7.0 EMPOWERING PARENTS AND EDUCATORS

While institutional mechanisms are crucial, no technical or legal solution can replace the role of informed, engaged parents and educators. Empowerment at the family and school level is the ultimate frontline defense for child online safety.

Mauritius must launch a national strategy to equip parents, guardians, and educators with practical knowledge and tools to supervise, guide, and support children in their digital journeys.

7.1 Digital Literacy Programs for Parents

A structured Digital Parenting Literacy Program should be launched in collaboration with NGOs, schools, religious organizations, and community centers. Key elements should include:

- **Workshops and Webinars:**

  Regular in-person and online sessions teaching parents how to:

  - Set up parental controls on devices and apps.
  - Understand platform risks (e.g., TikTok trends, WhatsApp scams, Discord servers).
  - Recognize signs of cyberbullying, grooming, or excessive gaming.

- **Bite-Sized Educational Content:**

  Short videos, podcasts, and infographics explaining key risks in under 3 minutes, distributed via:

  - SMS
  - Social media
  - School newsletters
  - Community WhatsApp groups

- **Hands-On Guides:**

  Step-by-step printed and online manuals in English, French, and Creole on:

  - How to configure YouTube Kids.
  - How to enable SafeSearch on Google.
  - How to report inappropriate content.

- **Digital Literacy Programs for Parents**

  In addition to personal device controls, parents should also be equipped with the skills to manage household-level internet safety. Training modules must include basic router configuration techniques, allowing parents to:

  - Set up content filters directly on home Wi-Fi networks;
  - Block access to specific websites or categories (e.g., adult content, gambling sites);
  - Schedule internet "downtime" periods during which devices cannot access the internet (e.g., after 10 p.m.);
  - Monitor traffic logs where appropriate to detect unusual or risky usage patterns.

  Providing parents with step-by-step guides and easy-to-follow video tutorials for popular router brands (e.g., Huawei, TP-Link, Netgear) can demystify this process and significantly enhance home-based child online safety.

  Moreover, collaboration with Internet Service Providers (ISPs) should be encouraged to offer user-friendly parental control dashboards bundled with standard household internet packages, making safe configuration easier for all households.

This network-level approach strengthens the safety net around children and empowers parents to manage risks proactively — not reactively.

Inclusivity must be prioritized, ensuring access for lower-income, rural, and non-tech-savvy families.

7.2 Parental Monitoring Tools and Alerts

Parents must be empowered through the deployment of transparent monitoring technologies:

- Usage Dashboards: Apps allowing parents to view children's online activity (without intruding on privacy when not necessary).
- Danger Hours Alerts: Notifications sent to parents if a minor is accessing internet services excessively at night (e.g., post 10 p.m.).
- Content Alerts: Warnings if minors attempt to access flagged content categories (violence, sexual content, gambling).

Importantly, parents must have the right to opt-in to deeper monitoring, respecting older minors' growing autonomy.

7.3 Digital Parenting Portal and Helpline Support

To strengthen parental engagement in child online safety, Mauritius should establish a national Digital Parenting Portal — an accessible online hub available in both Creole and English. The portal would offer:

- Practical, step-by-step guides for configuring privacy settings, enabling parental controls, and reporting inappropriate content;
- Short, relatable video lessons explaining online risks (e.g., social media dangers, gaming addiction, grooming warning signs);
- Regular updates on emerging trends in online threats affecting children.

Alongside the portal, a Parent Helpline should be established — offering telephone, SMS, and chat support for caregivers facing child online safety challenges. This Helpline could assist parents with:

- Guidance on how to respond to cyberbullying incidents;
- Immediate advice on how to report abusive content;
- Psychological first aid referrals for children impacted by online harm.

Social media campaigns and periodic WhatsApp blasts (e.g., “Tip of the Week”) can further drive awareness and usage of these resources. Schools, libraries, and community centers should promote the portal and Helpline widely, embedding them into national child protection outreach programs.

Providing parents with accessible, continuous, and real-time support strengthens the overall ecosystem of digital protection and empowers families to be proactive partners in safeguarding children online.

7.4 School-Led Initiatives

Schools should be empowered and mandated to:

- Incorporate mandatory digital citizenship modules into the curriculum by Grade 6.
- Host Parent-Teacher Digital Safety Days at least twice a year.
- Collaborate with COPA to deliver certified digital safety training for educators.

Schools must serve as bridging institutions between children, families, and state initiatives.

7.5 National Digital Awareness Campaign

Mauritius should launch a sustained, engaging public awareness campaign:

- Television and radio advertisements.
- Billboards highlighting dangers like grooming and gambling.
- Partnerships with influencers and celebrities to deliver messages on safe digital behavior.
- Special “Online Safety Weeks” celebrated nationally, focusing on different themes: cyberbullying, data privacy, digital wellbeing.

Messaging must be positive, empowering, and focused on digital opportunities and resilience, not fearmongering.

8.0 CHILD EDUCATION AND SENSITISATION

True digital safety begins with the child. Building digital resilience must be an integral part of growing up in Mauritius. A structured national program of age-appropriate sensitisation and capacity-building should be launched to educate children at every developmental stage.

8.1 Age-Appropriate Digital Education

Digital education must be introduced progressively, adapted to the maturity and psychological understanding of children.

Age Group	Key Focus Areas
6–9 years	Introduction to basic internet concepts: what is the internet; what is private information; basic online manners ("netiquette").
10–12 years	Safe search habits; understanding advertisements; dealing with strangers online; basics of cyberbullying awareness.
13–15 years	Online consent; digital footprint; privacy settings on social media; identifying grooming behavior; recognizing manipulation and fake news.

16–18 years	Responsible digital citizenship; peer influence; critical thinking regarding online content; advocacy for safer online communities.

Content should be localized in English, French, and Creole, and delivered via interactive methods such as videos, games, role-play exercises, and school projects.

8.2 Integration into School Curricula

Mandatory inclusion of Digital Safety Education Modules into:

- Civics classes
- Information and Communication Technology (ICT) curriculum
- Personal and Social Education (PSE)

National guidelines should standardize the core competencies expected at each educational level. Assessment (quizzes, small projects) can reinforce knowledge retention without creating additional high-stakes pressure.

8.3 Peer-to-Peer Education Initiatives

Students tend to trust and respond better to their peers. Mauritius should encourage:

- Digital Ambassadors programs, where older students are trained to mentor younger students on online safety.
- School clubs focused on digital wellbeing.
- Online safety competitions (essays, videos, campaigns) with awards and national recognition.

This not only builds resilience but empowers children to become advocates for a safer digital environment.

8.4 Enhancing Educator Preparedness through CPD

Successful integration of digital safety education into the school curriculum requires that educators themselves are adequately trained to deliver sensitive and evolving content confidently and responsibly.

Mauritius should therefore implement a mandatory Continuing Professional Development (CPD) program for teachers focusing on:

- Understanding online risks faced by children at different ages;
- Effective pedagogical strategies for teaching digital resilience and citizenship;
- Recognizing signs of online exploitation, cyberbullying, or technology-related mental health issues among students;
- Knowing appropriate referral mechanisms if children disclose online harms.

These CPD modules should be:

- Updated regularly to reflect new trends (e.g., AI risks, emerging platforms);

- Developed in partnership with child online safety experts and aligned with international frameworks (e.g., UNESCO, UNICEF digital safety curricula);
- Delivered through accessible formats (workshops, online webinars, certification courses).

By empowering teachers through systematic digital safety training, Mauritius will ensure that online protection messages are reinforced at every level of children's educational experience — and that schools become proactive environments for digital resilience building.

8.5 Nationwide Awareness Through Popular Media

In parallel to formal education:

- Short educational clips should be aired before children’s TV programs and YouTube content.
- Comics, animation series, and online games with embedded online safety messages should be developed.
- Interactive online challenges (e.g., "Stay Safe Online" quests) can gamify positive behavior.

Messaging should frame digital safety positively: not about fear, but about empowerment, autonomy, and respect for self and others.

9.0 MANAGING PLATFORM RESPONSIBILITIES

No child online safety framework can succeed without the direct participation of online service providers — particularly social media platforms, gaming companies, and search engines. However, platform responsibility must be regulated carefully, balancing enforcement needs against risks of overreach and abuse.

Mauritius must implement a "Smart Regulation" approach: firm, clear rules — but without arbitrary censorship or undermining fundamental freedoms.

9.1 Legal Duty of Care for Platforms

Platforms accessible to Mauritian users must be subject to a legal duty of care toward minor users. This would include obligations to:

- Design platforms with child safety in mind (safety-by-design standards).
- Prevent access by underage users through enforced, verified age checks.
- Provide age-appropriate content filters and user settings by default.
- Limit addictive design features (e.g., infinite scroll, autoplay for under-18 accounts).

The duty of care model draws inspiration from the UK’s Online Safety Act 2023 but must be adapted to avoid bureaucratic overcomplexity that could harm small innovators in Mauritius.

9.2 Enforced Compliance via Local Representation or Legal Agents

Given that many major platforms have no local offices in Mauritius, the law should require:

- Platforms with more than a threshold number of Mauritian users (e.g., 10,000 active users) must appoint a local legal agent responsible for compliance.
- Local agents can be served with takedown notices, court orders, and compliance audits.
- Non-compliance by platforms should trigger graduated penalties, escalating from fines to temporary service blocks for the Mauritian market.

This mirrors successful mechanisms in Australia and Germany.

9.3 Institutionalizing Safety by Design Compliance

To proactively protect minors online, Mauritius should mandate that Safety by Design principles are embedded into all platforms and digital services accessible to Mauritian users.

This would require online platforms, social media companies, app stores, and device manufacturers to:

- Default privacy settings to the highest protection level for users under 18;
- Prohibit algorithmic promotion of adult, violent, gambling, or otherwise harmful content to minors;
- Ensure age verification mechanisms are robust, secure, and effective, particularly before granting access to sensitive services or content;
- Provide clear, user-friendly abuse reporting mechanisms prominently accessible to minors;
- Disable addictive design features (e.g., infinite scroll, autoplay videos) for users under a designated age threshold.

Platforms meeting these standards should be audited annually and required to submit Child Safety Compliance Reports to the Child Online Protection Authority (COPA). Non-compliance should trigger warnings, sanctions, or restricted access measures under Mauritius' digital governance framework.

Embedding child safety at the design stage significantly reduces downstream risks and shifts responsibility back onto tech companies — ensuring that protecting young users is not left solely to parents or regulators.

9.4 Transparent Content Takedown Frameworks

Platforms must be required to:

- Publish clear community standards outlining prohibited content (child sexual abuse material, grooming, cyberbullying, hate speech targeted at minors).
- Set up swift complaint mechanisms accessible to Mauritian users.

- Respond to verified complaints within 24–48 hours.
- Notify complainants about the resolution of their complaints.

All takedown requests initiated by Mauritius' Child Online Protection Ombudsman (COPA) must be processed within 24 hours, with appeals possible through judicial review to protect free expression.

9.5 Expanding Technical Protection Measures for Families

Technical safeguards must complement legal reforms and educational initiatives to create a safer digital environment for Mauritian children. Mauritius should promote the nationwide deployment of free family-safe DNS filtering services, in partnership with providers such as OpenDNS FamilyShield and Google SafeSearch. Public education campaigns should encourage households to easily configure their home Wi-Fi routers to block adult content, gambling sites, and known harmful domains.

Internet Service Providers (ISPs) should be encouraged — or legally required — to offer "Family Safe" internet bundles with pre-activated content filtering as the default setting, giving families safer browsing environments without technical complexity. On the hardware side, device retailers should be incentivized to promote child-appropriate smart devices, such as:

- Low-cost "KidSmart" tablets preloaded with educational apps and strong content filters;
- Smartphones and tablets with Child Mode settings pre-activated out-of-the-box;
- Devices designed with robust parental management apps easily accessible to caregivers.

Where feasible, the government could negotiate public-private partnerships with major manufacturers (e.g., Samsung, Apple, Huawei) to make affordable child-friendly devices available through school programs or national initiatives.

By embedding protection at the network and device levels, Mauritius can create an ecosystem where children's exposure to online risks is minimized even before problems arise.

9.6 Protection Against Misuse of Content Moderation Powers

To prevent censorship creep:

- Content removal policies must focus narrowly on protecting minors from objectively harmful material.
- Platforms must maintain public transparency reports, disclosing:
  - Number of content removals;
  - Categories of content removed;
  - Source of removal requests (government, users, internal platform actions);
  - Appeals statistics and outcomes.

Transparency will serve as a deterrent against political misuse and reinforce trust in the system.

9.7 International Cooperation

Mauritius must strengthen its participation in international digital governance bodies (e.g., WePROTECT Global Alliance, Internet Watch Foundation) to:

- Share intelligence on online child abuse material (OCAM).
- Access cross-border cooperation channels for content removal outside local jurisdiction.
- Influence evolving international norms to better reflect small island state concerns.

10.0 IMPLEMENTATION ROADMAP

Adopting a comprehensive child online safety framework requires careful, phased implementation. Mauritius must sequence its efforts to build momentum, deliver early successes, and maintain long-term institutional resilience.

A realistic three-phase roadmap is recommended:

10.1 Phase 1: Immediate Actions (0–6 Months)

(a) Legislative Preparation

- Draft and publish a Child Online Protection Bill including:
  - Digital Age of Consent provisions.
  - Platform legal obligations.
  - Parental empowerment measures.
  - Establishment of the Child Online Protection Ombudsman (COPA).
- Amend the Cybersecurity and Cybercrime Act 2021 to reference COPA powers.

(b) Institutional Setup

- Create the Office of the Child Online Protection Ombudsman (temporary Secretariat under Ministry of ICT until independent).
- Establish initial reporting mechanisms (SMS hotline, basic web portal).

(c) Launch Public Awareness Campaign

- National campaign targeting parents, children, and educators on basic digital safety.

(d) Engage Platforms and ISPs

- Open formal consultations with major platforms (Meta, Google, TikTok, etc.) to align on expectations.
- Issue initial voluntary codes of practice while preparing binding regulations.

10.2 Phase 2: Short-Term (6–18 Months)

(a) Full Enactment of Laws

- Pass the Child Online Protection Act.
- Operationalize the Ombudsman's full investigative and enforcement powers.
- Publish regulations mandating age verification, platform accountability, and data minimization for minors.

(b) Capacity Building

- Recruit and train a team for COPA: investigators, case managers, digital analysts.
- Launch accredited Digital Safety Training programs for school teachers, counselors, and police.

(c) Build Partnerships

- Sign MOUs with international organizations (e.g., WePROTECT, IWF).
- Establish direct referral mechanisms with social media companies for faster abuse takedowns.

(d) Expand Educational Programs

- Roll out Digital Citizenship modules in primary and secondary school curricula.
- Launch the National Digital Parenting Portal with bite-sized guides, webinars, and a hotline.

10.3 Phase 3: Medium-Term (18–36 Months)

(a) Advanced Enforcement and Accountability

- Enforce mandatory reporting obligations for platforms.
- Publish annual Child Online Safety Reports (with statistics, performance grading for platforms).

(b) Full Local Presence Requirements

- Require major platforms exceeding user thresholds in Mauritius to appoint local legal representatives.
- Begin administrative penalty proceedings for non-compliant platforms.

(c) Deepen Child Protection Culture

- Establish "Digital Safety Ambassadors" programs in schools.
- Conduct nationwide Digital Literacy Surveys to track progress and identify gaps.

(d) Evaluate and Adapt

- Commission an independent review of the child online safety framework after 2 years.

- Update laws and regulations as needed to reflect new technologies, threats, and lessons learned.

10.4 Monitoring, Evaluation, and Agile Policy Adaptation

A strong and adaptive monitoring and evaluation framework is essential to ensure that Mauritius' child online safety strategy remains effective, accountable, and future-proof.

An inter-ministerial Child Online Safety Taskforce should be established, bringing together representatives from MITCI, the Ministry of Education, the Ministry of Gender Equality, law enforcement, civil society, and technical experts.

This Taskforce should meet bi-annually to review:

- Complaint data from MAUCORS+ and the Parent Helpline;
- Cybercrime incident reports involving minors;
- National surveys on children's digital habits and safety perceptions;
- Emerging technological trends or new online risks.

Mauritius should publish an Annual Child Online Safety Report, presenting key metrics publicly, including:

- Number of online harm cases reported and resolved;
- Levels of school-based incidents (e.g., cyberbullying reports);
- Progress on platform compliance;
- Public engagement with digital parenting resources.

The strategy must follow a Living Policy model:

Measures and regulations should be reviewed and adapted dynamically based on real-world data and changing technologies (e.g., new social media trends, AI-driven threats). Youth voices should be systematically included through a Youth Digital Safety Advisory Panel, ensuring that reforms are informed by those most affected.

By embedding continuous evaluation and agile policy mechanisms, Mauritius can maintain leadership in child online protection and rapidly respond to emerging challenges in the digital ecosystem.

10.5 Key Milestones

Milestone	Target Date
Draft Child Online Protection Bill	Month 3
COPA Secretariat operational	Month 6
First public education campaign launched	Month 6
Full legislation passed and enacted	Month 12

Platform compliance codes in force	Month 15
First Annual Child Online Safety Report	Month 24

11.0 EXPECTED OUTCOMES AND BENEFITS

Implementing the proposed Child Online Safety Framework will not only safeguard the digital lives of Mauritius' children, but will also foster broader societal, economic, and governance improvements.

11.1 Direct Benefits for Children

- **Increased Safety:**
  Children will be protected from online grooming, cyberbullying, predatory content, and exposure to harmful materials.
- **Empowerment and Resilience:**
  Through education and guided usage, children will develop digital literacy skills essential for 21st-century life, including critical thinking, privacy management, and respectful communication.
- **Mental Health Protection:**
  Reducing exposure to toxic environments, online harassment, and addictive platform mechanics will support better mental health outcomes among young users.

11.2 Benefits for Parents and Families

- **Increased Parental Engagement:**
  Parents will gain the tools and knowledge needed to guide and protect their children online, fostering stronger family bonds around digital life.
- **Peace of Mind:**
  Clear, standardized protections will reduce the anxiety parents often feel about their children's online activities.

11.3 Societal and Educational Benefits

- **More Trustworthy Digital Ecosystem:**
  Through strengthened standards and transparent enforcement, Mauritius can foster a safer, healthier national digital space for all users — not only children.
- **Improved Educational Outcomes:**
  By reducing distractions, exposure to harmful content, and negative peer pressures online, students will be better positioned to focus on their education and academic performance.
- **Fostering a Culture of Responsibility:**
  Training youth in digital ethics, citizenship, and critical thinking will contribute to a more respectful, tolerant, and informed society.

11.4 Economic and Innovation Benefits

- **Trust as a Competitive Advantage:**
  Mauritius can market itself internationally as a safe, child-friendly digital hub, attracting ethical tech companies, educational platforms, and international NGOs.
- **Reduced Social Costs:**
  Long-term public health and legal system burdens associated with cybercrimes, online addictions, and digital-related mental health issues will be mitigated.

11.5 Governance and Rule of Law Strengthening

- **Demonstrating Rights-Based Governance:**
  By embedding freedom of expression safeguards and transparent oversight mechanisms, Mauritius will reinforce its international image as a democracy committed to human rights in the digital age.
- **Compliance with International Norms:**
  The framework aligns Mauritius with leading standards advocated by UNICEF, ITU, the WePROTECT Global Alliance, and the United Nations' child rights guidelines.

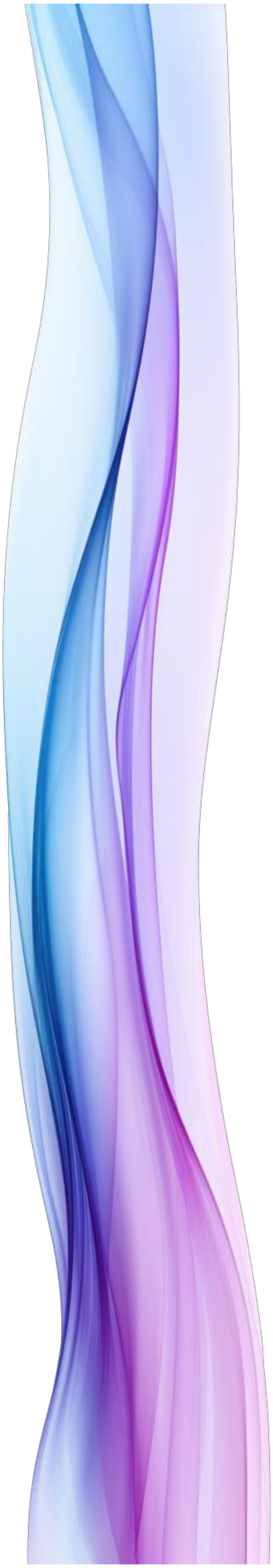
12.0 CONCLUSION

The internet will remain a defining feature of the lives of Mauritian children, shaping their education, friendships, entertainment, and even their future careers. Yet without a robust, forward-looking, and rights-respecting framework, it also exposes them to unprecedented risks.

This report has laid out a comprehensive strategic framework tailored for Mauritius — combining legal reforms, institutional innovations, education programs, technological solutions, and parental empowerment. It emphasizes that protecting children online is not solely a matter of restriction; it is fundamentally about building capacity, preserving dignity, and nurturing autonomy. Importantly, the proposed approach strikes the necessary balance between safety and freedom. It upholds freedom of expression, ensures judicial oversight, and resists the temptation of unchecked censorship, reaffirming Mauritius' commitment to democratic values in the digital era.

The time to act is now. As technology evolves rapidly, inaction or piecemeal efforts will leave Mauritian children vulnerable, while undermining trust in the digital society. With decisive leadership, collaborative spirit, and a clear focus on empowering the next generation, Mauritius can become a regional and global model for how to protect children online — without sacrificing rights, innovation, or opportunity. It is hoped that the policymakers, educators, technology companies, parents, and the broader Mauritian society will join forces to build a digital environment where every child can thrive safely, confidently, and freely.

ABOUT ILMA FOUNDATION



ILMA Foundation is a foundation registered under the laws of Mauritius (the “Foundation”).

The Foundation is a charitable foundation.

The Purpose and Object of the Foundation is to:

i. alleviate poverty,

ii. advance in education,

iii. assist in the development of religion,

iv. preserve of the environment,

v. protect the fundamental human rights in Mauritius, in the Indian Ocean and in Africa.

CONTACT US

contact@ilmafoundation.com
+230 5251 5351
http://www.ilmafoundation.com

ilma Foundation

Appendix 1 – Countries Analysis

Appendix 2 – References

CONTENTS

1.0 INTRODUCTION

Mauritius is witnessing a sharp rise in children's use of social media and online platforms, bringing tremendous opportunities for learning and connection – as well as new threats that demand urgent action. Recent incidents involving cyberbullying, exposure to explicit content, and online predation have underscored the social, emotional, and mental health impacts of unsafe online experiences. The Government of Mauritius has recognized the gravity of this challenge. In April 2025, the Ministry of Information Technology, Communication and Innovation (MITCI) released a draft Child Online Safety report and invited public consultation on measures to create a more secure digital environment for children and adolescents. The press notice (above) emphasizes that broad stakeholder input – from parents, educators, youth, tech companies, and civil society – is needed to ensure the final policy reflects community needs. This collaborative approach aligns with global trends: effective child online protection requires the involvement of all stakeholders, public and private (Today, 2021).

At its core, *child online safety* refers to safeguarding children (persons under 18) from dangers in the digital environment. These dangers span content risks (e.g. pornography or violent media), contact risks (undesired adult solicitation or grooming), conduct risks (cyberbullying, hate speech), and contract/consumer risks (fraud, in-app purchases, privacy violations) (THE AFRICAN UNION, 2024). The impacts are multi-dimensional – legal (e.g. criminal exploitation), technological (malicious content and algorithms), educational (digital literacy gaps), social (peer and community norms online), and psychological (mental health effects like anxiety or low self-esteem). Addressing such a complex issue necessitates a comprehensive, multi-pronged strategy. This report first examines successful approaches from other countries – Singapore, the United Arab Emirates (UAE), Malaysia, China, several African nations, and Scandinavian countries – to distill best practices and lessons on measuring effectiveness. It then discusses the pivotal role of parental education and community engagement in prevention, alongside specific technological tools (like router-based filters and safer device design) that can help protect children. Finally, evidence-based recommendations are presented for Mauritius, mapping a path toward an integrated policy framework that ensures children can benefit from the digital world safely.

2.0 INTERNATIONAL PERSPECTIVES ON CHILD ONLINE SAFETY

Around the world, governments have adopted diverse strategies to protect children online. Some focus on strict regulation and enforcement, while others emphasize education and empowerment, and many employ a mix of both. Below, we compare approaches in selected countries and regions – highlighting their successes and how they monitor and evaluate the impact of their interventions.

2.1 Singapore: Codes of Practice and Ratings for Platforms

Singapore has developed one of the most robust regulatory regimes for online safety. In 2023, it enacted the Online Safety (Miscellaneous Amendments) Act to require major online services to keep their platforms safe for users, especially children. Under Codes of Practice for Online Safety, designated social media services must: minimize exposure to harmful content (through content moderation and proactive removal of child sexual abuse material or grooming content), provide extra protections for children's accounts, implement age verification to prevent underage app downloads, and offer easy tools for users to report abuse. Notably, Singapore directly holds platforms accountable by mandating Annual Online Safety Reports. Each year, social media companies like Facebook, TikTok, and YouTube must report on their child safety measures, which the regulator assesses for comprehensiveness and effectiveness. In the inaugural 2024 assessment, the authority gave each platform safety ratings, finding that while general user safety and transparency were fairly strong, several platforms "did not do as well in user safety measures for children and in user reporting and resolution". By publishing these ratings and reports, Singapore empowers users (including parents) to make informed choices about which services are safest. This rigorous monitoring drives continuous improvement: companies face public scrutiny and are pressed to enhance child protections year over year. Beyond regulation, Singapore also invests in public education through its "Digital for Life" movement, uniting government, industry and community to improve digital literacy and wellbeing for all citizens. In summary, Singapore's approach combines strict enforcement (backed by the ability to direct removal of egregious content like child exploitation material) with transparency and education, and it measures success via annual audits and safety scorecards for platforms (Anon., n.d.).

2.2 United Arab Emirates: National Campaigns and Legal Duties

The United Arab Emirates (UAE) has pursued a proactive strategy centered on nationwide awareness initiatives and supportive laws. In 2018, the UAE launched the *Child Digital Safety* campaign – a joint effort by the Ministry of Interior and the National Programme for Happiness & Wellbeing – to educate children about online threats and encourage safe, constructive use of the internet. This initiative rolled out four sub-programs: (1) an interactive camp teaching 5–18-year-olds how to use social media securely, (2) a Digital Wellbeing Portal with tools and information for parents on managing digital challenges, (3) training workshops for parents and teachers on confronting cyber threats, and (4) a support hotline to answer urgent queries from parents about online safety. The strong emphasis on parent and educator engagement reflects recognition that adults need the knowledge to safeguard children. Legally, the UAE has integrated child online protection into its framework. *Wadeema's Law* (Federal Law No. 3 of 2016 on children's rights) obliges telecom operators and ISPs to notify authorities of any child pornography material circulating and to provide data on offenders. This creates a duty to report and enables law enforcement to swiftly respond to online child sexual abuse. Dubai's Data Protection Law (2015) likewise bolsters privacy for all individuals, including minors. To address online gaming risks, the UAE's Sannif initiative helps parents understand game content ratings and their impact on children. The success of the UAE's approach is monitored in several ways. The government tracks outreach – e.g. number of students attending the camps, or parents using the Digital Wellbeing Portal – as indicators of increased awareness.

On the enforcement side, compliance with mandatory reporting (Wadeema's Law) and subsequent prosecution of offenders signal effectiveness. The UAE also aligns with global standards: it has adopted the International Telecommunication Union's 2020 Child Online Protection (COP) Guidelines, which provide best practices for children, parents, industry, and policymakers (Anon. n.d). By embedding global benchmarks and inviting international collaboration (the UAE is partnering on an AI initiative for child safety), authorities can measure their progress against international metrics. Overall, the UAE exemplifies a holistic approach blending education with enforcement. Its visible commitment – such as regularly updating the public (most recently in Feb 2024) on child online safety efforts– helps maintain momentum and trust in these measures (Minevich, M., 2023).

2.3 Malaysia: Strengthening Laws and Leveraging Research

Malaysia's strategy has evolved in response to research and emerging threats, with a strong focus on legal reform and evidence-based policy. In 2017, Malaysia passed the Sexual Offences Against Children Act, a law targeting child sexual exploitation, and in 2023 lawmakers introduced amendments to address new forms of abuse like *sexual extortion (sextortion)* and *live-streaming of child abuse*. This move came on the heels of a comprehensive national study, *Disrupting Harm*, which revealed alarming statistics – an estimated 100,000 Malaysian children aged 12–17 experienced clear instances of online sexual exploitation in just one year. The data showed that threats like sextortion were widespread, yet under-reported and not explicitly criminalized until the recent legal updates. By making sextortion and live-streamed abuse distinct offenses, Malaysia is enabling better prosecution of crimes that previously fell through gaps in the law (Anon., 2025c).

Malaysia also established specialized law enforcement capacity, such as the Malaysia Internet Crimes Against Children (MICAC) investigative unit, to tackle online child abuse. Success is measured by increased reporting and prosecution: early indicators suggest that clearer laws have empowered authorities to bring more cases to justice and have raised public awareness that such acts are punishable. For example, after outreach efforts, more victims have been willing to come forward, and police have noted an improved ability to categorize and pursue cases of online child sexual abuse. In terms of monitoring effectiveness, Malaysia collaborates with international initiatives and benchmarks. The government actively supported the Disrupting Harm study (led by UNICEF, ECPAT and Interpol), indicating a commitment to data-driven evaluation. The study's recommendations – spanning legislation, enforcement, justice, and social services – now serve as a blueprint against which Malaysia can track progress. For instance, one recommendation calls for monitoring the implementation of the 2017 law to identify obstacles hindering its effectiveness, effectively institutionalizing a feedback loop. Malaysia is also aligning national strategy with regional efforts, such as the ASEAN Regional Plan of Action on Eliminating Violence Against Children, and global frameworks like the WeProtect Model National Response. Each alignment provides external reference points (e.g. periodic ASEAN progress reviews, WeProtect's Global Threat Assessment) to measure success. In summary, Malaysia illustrates the importance of responsiveness to research: it identified gaps (like sextortion) through rigorous study and swiftly updated its policy response. By continuously evaluating outcomes – from how many victims use helplines to how courts handle new offenses – Malaysia aims to ensure its child online safety measures remain effective against evolving threats.

2.4 China: Strict Controls and Youth-Centric Tech Design

China has taken an assertive, state-driven approach to child online safety, often cited as the most stringent regulatory model. The Chinese government directly imposes limits on when and how minors can engage online, especially for gaming and streaming, to combat addiction and exposure to harmful content. Since 2019, regulations have progressively tightened: minors were first limited to 90 minutes of online games per weekday (and none late at night), and by 2021 China imposed an even stricter cap of only 3 hours of gaming per week (1 hour on Fridays, Saturdays, and Sundays). Enforcement is facilitated by required real-name registration and even facial recognition checks in some games to prevent youth from using adult accounts. Major apps and platforms are mandated to offer "Youth Mode" settings that limit screen time and filter content for underage users (Soo, 2023). To measure effectiveness, Chinese authorities rely on nationwide usage statistics and surveys of youth behavior. In 2022, a government-affiliated industry report declared that the gaming addiction problem among minors was "basically resolved," citing the fact that over 75% of minors now play less than 3 hours a week under the new rules. They also reported that most parents were satisfied with the restrictions and noted a decline in extreme gaming-related cases requiring treatment. These data points – reduced average screen time and positive parent feedback – are treated as indicators of success. Additionally, China tracks outcomes such as academic performance and health metrics (e.g. improvements in sleep patterns or eyesight among students) to see if the curfews and limits yield tangible benefits (Soo, 2023).

China's heavy content moderation and censorship infrastructure (the "Great Firewall") also means that many categories of harmful content (pornography, extreme violence, etc.) are broadly filtered for all users, indirectly protecting minors by default. The country augments this with targeted child protections: for example, popular Chinese social media platforms like Douyin (TikTok's counterpart) have a special mode for children under 14 that shows only educational content and blocks certain features. The effectiveness of these measures is monitored by the Cyberspace Administration through periodic inspections of platforms. Non-compliance can result in punitive action, so companies have internal teams to ensure content accessible by youth meets government standards. While these controls have indeed curtailed certain risks (Chinese officials reported a significant drop in underage gaming addiction cases year-on-year), they also present side effects – such as youth finding workarounds via VPNs or rented adult accounts. China acknowledges these challenges and continuously updates its approach (for instance, cracking down on account rentals and strengthening age verification technology). In conclusion, China's model shows that aggressive regulatory intervention can yield measurable reductions in specific online harms (e.g. gaming overuse), but it requires constant enforcement and technological reinforcement to maintain efficacy. The Chinese experience also underscores a cultural facet of success: broad social consensus (among parents, schools, and even youth themselves) around the importance of online discipline has facilitated implementation. Other nations may not replicate China's exact approach, but lessons can be drawn about linking policies to clear metrics (hours spent, content access rates) and investing in systems to monitor those metrics closely.

2.5 African Countries: Continental Frameworks and Emerging Initiatives

Across Africa, the landscape of child online safety policy is diverse, with many countries in the early stages of formalizing protections. However, significant progress is being made through regional collaboration and the adoption of common guidelines. In May 2024, the African Union (AU) became the first region in the world to implement a dedicated Child Online Safety and Empowerment Policy. This continent-wide policy framework outlines 10 key goals, ranging from strengthening legal and regulatory environments to ensuring corporate responsibility and investing in digital literacy education. By endorsing this policy, African governments have collectively recognized both the immense opportunities the internet affords youth and the urgent need to address associated risks. The AU policy defines online risks using the "4Cs" categorization (Content, Contact, Conduct, Contract risks) (Anon., n.d.), ensuring a comprehensive view that mirrors international child rights standards. Success for this regional approach will be measured through implementation at the national level: the AU is expected to monitor which member states enact laws or programs aligned with the 10 policy goals, and to facilitate knowledge-sharing of best practices between countries like Kenya, Ghana, Uganda, and Zambia, which already have documented safety initiatives (THE AFRICAN UNION, 2024).

At the country level, initiatives vary. South Africa, for example, has integrated online safety into its educational curriculum and runs awareness campaigns each Safer Internet Day, supported by a national safer internet centre. Kenya has a Child Online Protection (COP) framework under its Communications Authority, with guidelines for industry and outreach programs in schools. Nigeria and Zambia have partnered with mobile operators (like MTN) to research children's internet use and develop child-friendly services Bonisele, 2024. Many African nations leverage global support: for instance, Tanzania in 2022 launched a national child online safety strategy with support from the ITU, establishing a multi-stakeholder advisory council (Anon., 2025c). The effectiveness of these efforts is being tracked through both quantitative and qualitative means. Some countries conduct baseline and follow-up surveys on children's online behaviours and incidences of harms (e.g. % of youth encountering hate speech or being groomed). Others rely on proxy indicators such as hotline reports – for example, in South Africa, reports of online child sexual abuse material to the Film and Publication Board's hotline are monitored for trends. Regionally, the new AU policy implies that the AU Commission will likely collect data on member state progress and possibly establish an index or scorecard for child online safety in Africa. The mere creation of a unified policy is itself a success: as AU Commissioner Dr. Amani Abou-Zeid noted, "Africa pioneers... policy for protecting, empowering and ensuring the safety of children online" (Anon., 2025a).

This political will is a foundation on which measurable improvements (like increased awareness or reduced victimization rates) can be built.

That said, challenges remain in many African contexts, including limited digital literacy among parents, lower levels of technical infrastructure for monitoring, and cultural taboos around discussing sexual exploitation, which can hinder reporting. To address this, initiatives like Child Online Africa, an NGO, and the Africa Online Safety Platform are working to centralize resources and build capacity (Bonisele, 2024). In coming years, a critical marker of success will be how well African nations translate these frameworks into action – for example, updating a law to criminalize online grooming, or training law enforcement on cybercrime against children – and the extent to which children and parents report feeling safer and more informed online.

2.6 Scandinavian Countries: Education, Empowerment, and Support Systems

The Scandinavian nations (e.g. Finland, Sweden, Norway, Denmark) are often viewed as exemplars of child-centric digital policies with a focus on empowerment over restriction. These countries generally enjoy high internet penetration and digital literacy rates, and their approaches prioritize teaching children to navigate risks and providing support rather than heavy-handed censorship. Finland offers a strong case study: media and digital literacy education is woven into the national curriculum from an early age (Taruutriainen, 2024), and Finland's Safer Internet Centre provides resources and hotlines through organizations like the Mannerheim League for Child Welfare (Anon., 2021). Finnish children are taught in school how to critically evaluate online content, protect their privacy, and deal with issues like cyberbullying or stranger contact. Meanwhile, parents in Finland are encouraged to take an active role – not just by imposing rules, but by engaging in open dialogue about internet use. A recent Finnish survey found that children "explicitly wanted parents and schools to take on a more active role" in their digital lives, calling for parents to be trained on both the benefits and threats of online platforms. Indeed, children reported that many parents lack understanding of modern social apps or games and thus struggle to guide them. In response, NGOs and schools in Scandinavia frequently organize parent evenings and publish digital parenting guides to close this knowledge gap (Anon., n.d.).

The success of Scandinavian strategies is reflected in several metrics. According to pan-European studies (like EU Kids Online surveys), Nordic children tend to report high levels of digital skills and resilience – for example, knowing how to block unwanted contacts or configure privacy settings (Anon., n.d.). They also often have the confidence to seek help: thanks to the strong social support systems, children in these countries might be more likely to contact a helpline or tell a trusted adult when they encounter problems. Each country has a well-established helpline for youth (e.g. Sweden's Bris, Denmark's Cyberhus, Finland's Nettivihje for reporting online abuse), which logs thousands of cases annually and provides anonymized trend data to policymakers. Scandinavian governments monitor indicators such as the prevalence of cyberbullying. Notably, bullying (both online and offline) in some of these countries has declined or remained stable in recent years, contrary to fears of a cyberbullying "explosion" (Today, 2021). Experts attribute this in part to comprehensive anti-bullying programs in schools and a culture that promotes empathy and inclusion – showing that education and awareness can mitigate online risks. Moreover, privacy and data protection for children are strictly upheld (e.g. all Scandinavian countries enforce the EU's GDPR which has special provisions for children's data, and some have additional safeguards). A concrete innovation in Finland is the development of *AI tools to detect youth at risk*: Finland's government piloted an AI system called "Nuora" to identify signs of social media distress or exclusion among young users, which can enable early intervention (Anon., n.d.). This kind of forward-looking measure is evaluated by its accuracy and the successful support provided to identified teens.

In summary, the Scandinavian model emphasizes digital empowerment, mental well-being, and accessible support. These countries measure success less by blocking content (which they do to a limited extent in line with EU rules) and more by outcomes like children's self-reported safety skills, rates of harmful incidents, and help-seeking behaviour. The overarching philosophy is that a well-informed, resilient child – backed by involved parents and a safety net of school and community resources – is the best defence against online harms. This philosophy is increasingly influencing global thinking, complementing the more regulatory approaches seen elsewhere.

3.0 THE ROLE OF PARENTAL EDUCATION AND COMMUNITY ENGAGEMENT

A recurring theme across all successful child online safety strategies is the critical role of parents and caregivers. While governments can enact laws and companies can moderate content, day-to-day guidance and supervision of children's online activities largely fall to parents. However, many parents feel ill-equipped to deal with the fast-changing digital landscape that their children inhabit. Continuous Parent Development (CPD) programs – akin to professional development but for parenting in the digital age – can empower parents with the knowledge and skills to keep their kids safe online. Such programs typically cover understanding the popular apps and games children use, recognizing online risks (like grooming or cyberbullying), setting up parental controls, managing screen time, and open communication strategies.

The effective parent-focused training would include topics like understanding social media (e.g. what TikTok, Snapchat, Instagram are and what risks they pose), technical skills such as configuring parental controls on home Wi-Fi routers or devices, strategies for managing screen time and device use rules, and resources for parental support (like helplines or support groups). Delivering this education in a user-friendly manner is vital. Many countries leverage familiar channels – social media and community networks – to reach parents. For example, short informational videos and infographics (like the one above) can be shared via Facebook, WhatsApp, and YouTube, where parents in Mauritius are active. Community workshops can be organized at schools, community centres, or by local parent-teacher associations, creating a forum where parents learn hands-on and share experiences. The UAE's initiative of training workshops for parents (Anon., 2024) is a good model that Mauritius could emulate, perhaps using a train-the-trainer approach to reach different regions and languages.

The need for parental education is evidenced by research. A study across several countries found that children often believe their parents "don't have enough knowledge of the safety challenges" they face online. Children actually *want* clearer rules and guidance – they feel safer when parents set boundaries and discuss online life openly (Anon., n.d.). Thus, parental engagement should not be seen as a restriction by children, but rather as a mutual effort to ensure well-being. Moreover, increasing parents' digital literacy can directly reduce risks: informed parents are more likely to use available safety tools and talk to their kids about risky behaviours. OECD analyses note that the dissemination of Internet safety information to parents and teachers (such as Ireland's Webwise portal) has been an important measure in many countries to improve child safety (Today, 2021).

For Mauritius, introducing CPD programs for parents could involve multimedia campaigns in collaboration with organizations like UNICEF or local NGOs. Social media outreach can include weekly tips on child online safety, live Q&A sessions with experts (for instance, on Facebook Live), and testimonials from other parents. Community channels might involve integrating a digital safety module into existing parent meetings at schools or using community radio to discuss issues in local dialects. The goal is to meet parents "where they are" and provide practical, culturally relevant advice. Success of such programs can be measured through surveys (do parents feel more confident about online safety after participating?), the adoption rate of parental control tools, or even reductions in negative incidents reported by schools. One concrete recommendation is to create an online portal or mobile app specifically for Mauritian parents, aggregating guides, video tutorials, and a forum for questions – essentially a "one-stop shop" for digital parenting resources, updated continuously as new trends emerge.

Importantly, parental education should be an ongoing effort (continuous development), not a one-off. As children grow and new platforms arise, parenting approaches must adapt. A feedback mechanism (e.g. an online poll or suggestion box on the portal) can let parents indicate what topics they need more help with, ensuring the program stays responsive. By empowering parents alongside children, Mauritius can foster a safer digital environment based on awareness and engagement, rather than fear or disengagement.

4.0 TECHNOLOGY TOOLS: ROUTER-BASED CONTROLS AND CHILD-FRIENDLY DEVICES

While education and policies set the groundwork, technology itself offers powerful tools to protect children online. Two practical technological measures are particularly worth implementing in Mauritius: (1) easy-to-use parental controls at the network (router/ISP) level, and (2) standardizing or guiding the types of devices young children use to those with safety features and limited functionality.

4.1 Router-Based Parental Controls and ISP Filtering

One of the most effective points to filter or monitor internet content is at the source of the connection – the home router or the service provider. Modern Wi-Fi routers often come with parental control settings that can block categories of websites (pornography, gambling, violence, etc.), enforce safe search on search engines, or set time limits for internet use on a child's devices. Similarly, ISPs can offer network-level filtering that parents can opt into (or which could even be enabled by default with an opt-out option). For instance, in the United Kingdom all major broadband providers, under government encouragement, implemented default-on content filters for adult content; parents can choose to disable them, but if left in place they automatically block many harmful sites for all devices in the home (Jackson, 2022). This UK model has shown moderate success: awareness of ISP filtering among parents is fairly high (about 61% of parents surveyed knew about these tools) and roughly 27% of UK parents actually use network filters provided by ISPs. Additionally, over 70% of parents use some form of technical control (including device-level tools) to help keep their children safe online (Anon., 2022). These numbers indicate that while such tools are not universally utilized, a significant minority find them valuable – and critically, they are a *choice* available to all.

For Mauritius, ensuring that all ISPs and mobile network operators offer user-friendly parental control options should be a priority. ISPs could provide a simple dashboard or mobile app for subscribers to toggle categories of content on/off for child profiles, set Wi-Fi schedules (e.g. no internet after 9 PM for kids), and receive reports on attempted access to blocked content. The government can incentivize or mandate ISPs to provide these services (for example, as a condition of operating licenses or through a voluntary code). Moreover, public awareness campaigns can advertise these features so parents actually know how to activate them. A common challenge is that many parents either don't know these controls exist or find them too complicated. Lessons from other countries suggest that default-on filters (with easy opt-out for those who don't need them) result in much higher uptake than purely optional ones (Anon., 2022). However, default filtering raises debates on censorship and over-blocking (e.g. sometimes even harmless sites get blocked by accident) (Geigner, 2022). A balanced approach could be "nudging" during router setup or ISP sign-up – e.g. a prompt: "Do you have children in the household? Yes/No – if Yes, would you like to enable child-safe browsing mode?" This respects choice while encouraging protection. To measure effectiveness, Mauritius could track metrics like the percentage of families activating these controls and any correlation with reduced incidents (for example, do schools report fewer cases of children accessing inappropriate material from home?). The UK's Ofcom reports and others provide a template for such evaluation, noting not just usage rates but also instances of circumvention (in the UK, a small percentage of tech-savvy teens found ways around filters) (Geigner, 2022), which underscores that technology is not fool proof and should complement, not replace, parental oversight.

4.2 Child-Friendly and Standardized Devices

Another innovative recommendation is to standardize the type of mobile phones or devices used by young children to ensure they serve safety and learning, rather than distraction or harm. The ubiquity of smartphones means many children receive powerful internet-enabled devices at an early age – sometimes as early as primary school. Research suggests that early smartphone ownership can heighten risks: children as young as 8-11 who own phones have been found more likely to be involved in cyberbullying (as victims or perpetrators) compared to peers without phones. Also, excessive smartphone use is linked to problems like reduced attention span and sleep disruption in children (Smale et al., n.d.). To mitigate this, some countries and experts propose giving children simpler, purpose-limited phones (often dubbed "feature phones" or specially designed kids' smart devices) instead of full-fledged smartphones. For example, Japan for years has had kids' phones with GPS tracking and a whitelist of contacts; and France banned smartphones in schools up to 9th grade, effectively encouraging that children either have no phone or only a very basic one during school hours. Standardizing devices could mean that the Ministry of Education, for instance, works with telecom providers to introduce an affordable "kids' phone" that has built-in parental control software, no access to app stores without permission, and only essential apps (education, calling family). Alternatively, the policy could simply be strong guidance to parents that children under a certain age (e.g. 12) should not use unmanaged smartphones, coupled with recommendations of vetted products or settings.

In Mauritius, one approach could be implementing a program through schools where, if a student needs a device for communication, the school facilitates the purchase of a pre-configured tablet or phone that has standardized safety settings. This could ensure that all students have a device that blocks adult content, limits screen time, and allows monitoring of usage by parents. Not only does this protect the child, it also ensures more equitable access to technology for learning (since the device can be chosen with educational utility in mind). Standardization doesn't necessarily mean one model for all, but rather a set of minimum safety requirements for any device used by children: for example, "any smartphone given to a child must have [a] web filtering enabled, [b] usage time limits, [c] no social media apps for under-13 users except those with parental approval, etc." Manufacturers and mobile operators can be brought into a discussion to support these guidelines (possibly introducing a "child-friendly device" certification).

Effectiveness of such a measure can be observed in reduced distraction and cyber incidents in school settings. If students use only vetted devices, teachers might report fewer issues with inappropriate content being shared. Parents may also notice positive effects – one study cited a substantial improvement in test scores when phones were banned in schools, benefiting especially previously low-achieving students. In Mauritius, where academic performance is a key concern, limiting smartphones could have dual benefits: safety and improved concentration on studies. To avoid backlash, it's important that any standardization policy be accompanied by public awareness explaining the rationale (for instance, sharing evidence that younger children with unrestricted smartphones face higher cyberbullying risks and mental health issues). By framing it as ensuring devices are *age-appropriate* rather than a ban, parents are more likely to be receptive. Over time, as the child matures and demonstrates responsibility, privileges can be expanded – but the initial safe foundation is crucial.

In conclusion, deploying technical solutions like network filters and encouraging safer devices can significantly reduce the exposure of children to online harms. These tools act as a front-line defence – filtering out the worst content and restricting dangerous functionality – while education and parental engagement deal with subtler issues that technology cannot solve alone. Mauritius should integrate these technology measures into its national strategy, working closely with ISPs, hardware/software providers, and regulators to ensure they are accessible, effective, and updated with the latest technological advancements.

5.0 POLICY RECOMMENDATIONS FOR MAURITIUS

Drawing together the insights from international best practices and the current gaps in Mauritius, this section outlines a proposed multi-dimensional policy framework for child online safety. The recommendations address legal reforms, institutional setup, education initiatives, technological tools, and collaboration mechanisms. Implemented together, they form a cohesive strategy to protect children online while empowering them and their guardians with the skills and tools for safe digital participation. Key recommendations include:

5.1 Establish a Dedicated Child Online Safety Authority

Create a national authority or commission (e.g. a *Child Online Protection Authority*) under MITCI to coordinate all efforts related to online child safety. This body would oversee implementation of policies, continuously monitor the digital environment for emerging risks, and ensure platforms abide by local regulations regarding child protection. It should have enforcement powers to investigate and sanction violations (for example, ordering takedowns of harmful content or penalizing non-compliant service providers). Having a central authority can improve accountability and streamline efforts that currently span multiple agencies. This authority can also serve as the national liaison to international initiatives like the WeProtect Global Alliance, ensuring Mauritius stays aligned with global best practices.

5.2 Strengthen Legal Frameworks and Enforcement

Review and update Mauritian laws to fill any gaps related to online offenses against children. This includes explicitly criminalizing online grooming, sexual extortion, and distribution of child sexual abuse materials (CSAM) if not already clear in existing law. Laws should also mandate that ISPs and digital platforms report any identified child exploitation content to authorities (similar to UAE's Wadeema's Law) (Smale et al., n.d.). Introduce legal requirements for tech companies to implement Safety by Design – for instance, requiring robust age verification for adult content sites or default privacy settings on apps for minors (Anon., n.d.). Additionally, empower law enforcement with training and resources to tackle cybercrimes against children (e.g. expand the cybercrime unit and ensure they have forensic tools for the dark web). Enforcement should be victim-centric – procedures like using child-friendly interview techniques and providing psychological support for child witnesses should be standardized (following recommendations from the Disrupting Harm project). Monitoring effectiveness: track the number of investigations, prosecutions, and convictions of online child exploitation cases as a metric of law enforcement capability; also monitor if reporting of incidents by the public increases (which would indicate greater awareness and trust in the system).

5.3 Adopt a "Safety by Design" Mandate for Industry

Work with social media companies, telecom operators, and device manufacturers to adopt industry codes of practice that protect children. This could mirror Singapore's approach of requiring platforms to *proactively* filter harmful content and provide stronger safety settings for minors (Anon., n.d.). For example, require that any social media service with significant Mauritian youth users must have: default privacy for under-18 accounts, no algorithmic promotion of adult content to minors, and easily accessible reporting mechanisms for abuse. App stores should enforce age ratings (preventing kids from downloading 18+ apps). Telecommunication companies should assist in blocking blatant illegal content (like known child abuse URLs) at the network level. By institutionalizing Safety by Design, the onus is partly on companies to create a safer environment, reducing the burden on users to constantly police what children see. The WePROTECT Global Alliance model encourages such public-private collaboration, and Mauritius should become an active member, committing industry partners to its standards. Effectiveness can be measured by auditing compliance (e.g. annual safety reports from companies, similar to Singapore's reporting requirement) and by outcomes (do user reports of harmful content decrease on platforms that implement new protections?).

5.4 Promote Digital Literacy and Resilience Education

Integrate comprehensive digital citizenship and online safety education into school curricula at all levels. Starting from primary school, students should learn age-appropriate lessons about online etiquette, privacy, recognizing misinformation, and handling cyberbullying. By secondary school, modules on topics like mental health in relation to social media, critical thinking about online influences, and understanding one's digital footprint should be included. The Ministry of Education can incorporate these into existing ICT or Life Skills classes, or as special sessions during the year (for example, around Safer Internet Day). Teachers will likely need training (Continuing Professional Development) to deliver this content confidently. Partnering with NGOs or using materials from UNESCO/UNICEF can provide localized yet high-quality content. Community-based programs are also important to reach out-of-school youth – for instance, library workshops or youth club activities focusing on online safety. A specific recommendation is to hold annual school campaigns or competitions on digital safety (such as poster contests, debates, or hackathons to create digital safety apps), which engage students creatively and reinforce knowledge. Measures of success: include questions about online safety in national assessments or surveys to see if knowledge is improving; monitor if schools report fewer incidents of cyberbullying year on year; possibly measure students' self-reported confidence in dealing with online risks before and after these interventions.

5.5 Launch Parental CPD Programs via Social Media and Communities

As detailed in the previous section, Mauritius should initiate a nationwide Digital Parenting campaign. This can involve an online portal in Creole and English with guides for parents, a series of short video lessons distributed on social media, and in-person community meet-ups. Government ministries (MITCI alongside Ministry of Gender Equality, Child Development and Family Welfare) can collaborate with telecom providers to send out periodic SMS/WhatsApp blasts with parenting tips (for example, "Tip of the Week: How to enable YouTube Restricted Mode to filter content"). Encourage schools to host parent orientation evenings about online safety at least once per year, possibly led by a trained facilitator. Additionally, consider setting up a Parent Helpline (or expanding an existing child helpline to also cater to parents) where caregivers can call for advice on dealing with online issues – whether it's a case of cyberbullying, or simply how to configure a tablet for a 10-year-old. This echoes the UAE's approach of a support platform for parent queries (Anon., 2024). We recommend evaluating these efforts by tracking attendance/participation numbers (e.g. how many parents join the Facebook Live sessions or community talks) and conducting feedback surveys. The ultimate indicator would be parents reporting greater confidence and actual changes at home (like more frequent conversations with kids about their online life, or increased use of parental controls – a metric that ISPs could help provide anonymized data on).

5.6 Enhance Technical Tools for Protection

Implement the technology measures discussed – notably, require ISPs in Mauritius to offer free parental control services (with clear how-to instructions for users) and consider making the "default on" filtering of adult content a standard, while respecting user choice to opt out (Anon., 2024). This might involve regulatory guidance from the ICT Authority. Also, work with internet router vendors to ensure that routers sold in Mauritius have parental control features accessible via a simple mobile app. A possible initiative is a government tie-up with a DNS filtering service (like OpenDNS FamilyShield or Google SafeSearch) to provide an easy one-click solution for homes to block known adult domains. On the device front, issue guidelines or an advisory to retailers and parents on child-appropriate devices. For example, encourage the sale of low-cost "KidSmart" tablets preloaded with educational content and strong filters, or push smartphone OEMs to include a "child mode" that parents can enable out-of-the-box. If feasible, negotiate with manufacturers (like Samsung or Apple) for special pricing on tablets for school programs, ensuring those come with management software. Over time, aim for a situation where it's normalized that a primary school child in Mauritius might have a basic phone or tablet that is intentionally limited and supervised, rather than an unrestricted smartphone. The government can even showcase examples – e.g. pilots where students in a few schools use a standardized tablet safely for a year, demonstrating better learning outcomes and no internet misuse, to persuade the public of the benefits.

5.7 Bolster Reporting Mechanisms and Support Services

Even with all preventive measures, some children will encounter harmful situations online. Strengthening reporting and response is thus crucial. Mauritius already has the Cybercrime Online Reporting System (MAUCORS+) for the public to report cyber incidents. This system should be adapted to specifically allow child-friendly reporting of online issues – possibly a dedicated section or a simplified interface for youth. It should also categorize incidents reported involving minors (cyberbullying, exploitation, exposure to illegal content, etc.) so that data on these are collected. We recommend establishing a 24/7 hotline (phone, text or chat) for children facing online harassment or abuse, staffed by counsellors trained in handling youth issues. This could build on existing child helplines in the country, augmenting them with an online safety specialization. Additionally, strengthen ties with international hotlines (like INHOPE network or NCMEC) to receive and share reports about child sexual abuse material online – this ensures Mauritius is plugged into global efforts to take down such content quickly. Ensure that whenever a report is made (either via MAUCORS+ or the hotline), there is a clear referral pathway: serious cases go to law enforcement; cases of psychological distress get referrals to mental health services (e.g. a youth psychologist); cases at school are flagged to the school authorities for follow-up, etc. Success can be measured by increased usage of these channels (a paradoxical but positive sign – as awareness grows, more reporting usually occurs before eventually declining as issues are prevented). Also track response times and resolutions – e.g. how fast inappropriate content reported by a parent is removed, or how many counselling sessions result from hotline calls. A qualitative measure of success is trust: children and parents should come to *view these services as safe, confidential, and helpful*. Outreach in schools and media should promote these resources regularly to embed them in public consciousness.

5.8 Monitor, Evaluate, and Iterate

Finally, embed a strong monitoring and evaluation framework in the policy implementation. This means setting up an inter-ministerial committee or taskforce that meets, say, bi-annually to review data on various indicators: number of complaints, surveys of children's digital habits, feedback from schools, crime stats, etc. Use this to produce an Annual Child Online Safety Report for Mauritius, summarizing progress, much like Singapore's annual safety assessments. This report should be public and transparent, highlighting achievements (e.g. "X% of schools now have digital safety classes, Y number of parents engaged, Z cases of cyberbullying handled") and challenges (areas where targets were not met). Solicit feedback from youth themselves – perhaps via a Youth Advisory Panel – to include children's voices in evaluating what's working and what's not (Ruhani, Elliot, and Australian eSafety Youth Council, 2023). By institutionalizing continuous improvement, Mauritius can adapt its strategy as technology and trends evolve. For example, if two years from now a new app is causing concern among kids, the taskforce can recommend actions swiftly rather than waiting for a crisis. This echoes the recommendation from WeProtect and OECD that policies must be agile and informed by up-to-date evidence (Today, 2021). In essence, treat the child online safety plan as a living policy: measure outcomes, get community input, refine measures, and update laws or programs accordingly.

6.0 CONCLUSION

Protecting children in the online sphere is a responsibility we all share – government, industry, educators, communities, and parents. Mauritius stands at an important juncture with the momentum building around child online safety and a recognition at the highest levels of its importance. By learning from global pioneers and tailoring solutions to the local context, Mauritius can develop a robust ecosystem of protections for young internet users. The evidence-based recommendations in this report chart a path forward: from updating laws and creating oversight bodies, to empowering children and parents through education and technological aids.

The overarching vision is to create a safe and empowering digital environment for Mauritian children. This means an internet where children are shielded from the worst dangers – sexual predators, extreme violence, hate – but not sheltered from opportunity. They can explore, learn, and socialize online with confidence because safety nets are in place: caring adults who are informed and involved, platforms that prioritize user safety in their design, and laws that have zero tolerance for those who harm or exploit minors. By implementing the proposed policy measures, Mauritius can significantly reduce online harms such as cyberbullying, exploitation, and exposure to inappropriate content, as evidenced by the successes seen in countries that have adopted similar multipronged approaches.

Crucially, this is not a one-time project but an ongoing commitment. The digital world will continue to evolve – new apps, new devices, new threats – and so must our strategies. Regular monitoring and community feedback will allow policies to stay effective and relevant. In parallel, nurturing open dialogues about online experiences – in families, in classrooms, in media – will help break the silence that often allows harm to fester. Children should feel heard and supported when they encounter difficulties online, and perpetrators must know that these issues are taken seriously by society.

In implementing these recommendations, stakeholders should also be mindful of children's rights and voices. Strategies should not simply be about restrictions, but also about respecting children's privacy and agency appropriate to their age. A rights-based approach, as advocated by UNICEF, emphasizes that children have the right to access information, to participation, and to be protected from harm – and these can be balanced in policy-making.

The challenge of child online safety is complex, but not insurmountable. With strong political will, cross-sector collaboration, and evidence-led action, Mauritius can become a leader in the region, perhaps even contributing to African and global knowledge on keeping children safe in the digital age. As one African proverb says, *“It takes a village to raise a child.”* In the 21st century, that village extends to the virtual realm. By raising our collective guardrails in that realm, we ensure our children can thrive both online and offline – confident, curious, and secure.

APPENDIX 2 - REFERENCES

Anon. 2021. *Finnish Safer Internet Centre - The Mannerheim League for Child Welfare*. [online] The Mannerheim League for Child Welfare. Available at: https://www.mll.fi/en/about-mll/media-education/finnish-safer-internet-centre/&gt; [Accessed 28 April 2025].

Anon. 2022. *A quarter of UK parents use content filters from broadband ISPs*. [online] ISPreview. Available at: https://www.ispreview.co.uk/index.php/2022/03/a-quarter-of-uk-parents-use-content-filters-from-broadband-isps.html&gt; [Accessed 19 April 2025].

Anon. 2024. *Child Digital Safety | the official portal of the UAE Government*. [online] Available at: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security/child-digital-safety&gt; [Accessed 19 April 2025].

Anon. 2025a. *Africa has become the first region in the world to implement a child online safety and empowerment policy | African Union*. [online] Available at: https://au.int/en/pressreleases/20240523/child-online-safety-and-empowerment-policy-africa-union&gt; [Accessed 19 April 2025].

Anon. 2025b. *Malaysia takes pivotal steps towards a safer internet for children following data from disrupting harm – Safe Online*. [online] Available at: https://safeonline.global/malaysia-takes-pivotal-steps-towards-a-safer-internet-for-children-following-data-from-disrupting-harm/&gt; [Accessed 19 April 2025].

Anon. 2025c. *Research - the Africa Online Safety Platform*. [online] Available at: https://www.africaonlinesafety.com/research#:~:text=Research%20,&gt; [Accessed 28 April 2025].

Anon. n.d. *Enhancing online safety in Singapore - Infocomm Media Development Authority*. [online] Infocomm Media Development Authority. Available at: https://www.imda.gov.sg/regulations-and-licensing-listing/content-standards-and-classification/standards-and-classification/internet/online-safety&gt;.

Anon. n.d. *Finland helps to safeguard child rights in the digital world - Finnish Government*. [online] Finnish Government. Available at: https://valtioneuvosto.fi/en/-/finland-helps-to-safeguard-child-rights-in-the-digital-world&gt;.

Anon. n.d. *Young people in Finland voice the need for media education*. [online] Better Internet for Kids. Available at: https://better-internet-for-kids.europa.eu/en/news/young-people-finland-voice-need-media-education&gt;.

Bonisele, 2024. *MTN advances online child safety efforts with new research and initiatives | MTN.com*. [online] MTN.com. Available at: https://www.mtn.com/mtn-advances-online-child-safety-efforts-with-new-research-and-initiatives&gt; [Accessed 19 April 2025].

Geigner, T., 2022. *They always suck: UK ISP "For the Children" filters block Disney and educational websites*. [online] Techdirt. Available at:

https://www.techdirt.com/2018/05/15/they-always-suck-uk-isp-children-filters-block-disney-educational-websites/&gt;.

Jackson, M. 2022, 'A quarter of UK parents use content filters from broadband ISPs - ISPreview UK', *ISPreview*, available at: https://www.ispreview.co.uk/index.php/2022/03/a-quarter-of-uk-parents-use-content-filters-from-broadband-isps.html [Accessed 28 April 2025].

Minevich, M., 2023. *Revolutionizing Child Protection: The UN and UAE's groundbreaking AI for Safer Children collaboration*. [online] Forbes. Available at: https://www.forbes.com/sites/markminevich/2023/12/26/revolutionizing-child-protection-the-un-and-uaes-groundbreaking-ai-for-safer-children-collaboration/&gt;.

Ruhani, Elliot, and Australian eSafety Youth Council, 2023. *Global Threat Assessment 2023*. [online] Available at: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf&gt;.

Smale, W.T., 1, Hutcheson, R., 2, Russo, C.J., 3, Trent University, McMaster University, and University of Dayton, n.d. *Cell phones, student rights, and school safety: finding the right balance*. [journal-article] Available at: https://files.eric.ed.gov/fulltext/EJ1287931.pdf&gt;.

Soo, Z., 2023. *China keeping 1 hour daily limit on kids' online games | AP News*. [online] AP News. Available at: https://apnews.com/article/gaming-business-children-00db669defcc8e0ca1fc2dc54120a0b8&gt;.

Taruutriainen, 2024. *Media Literacy and Education in Finland - Finland Toolbox*. [online] Finland Toolbox. Available at: https://toolbox.finland.fi/life-society/media-literacy-and-education-in-finland/&gt;.

THE AFRICAN UNION, 2024. *THE AFRICAN UNION CHILD ONLINE SAFETY AND EMPOWERMENT POLICY*. [policy] *44th Ordinary Session of the African Union Executive Council*. Available at: https://au.int/sites/default/files/documents/43798-doc-African_Union_Child_Online_Safety_and_Empowerment_Policy_Feb_2024.pdf&gt;.

Today, V.A.P. by O.E. and S., 2021. *Child safety in the digital age: How education systems can help*. [online] OECD Education and Skills Today. Available at: https://oecdedutoday.com/child-safety-digital-age-how-education-systems-can-help/&gt; [Accessed 19 April 2025].

United Nations Children's Fund (UNICEF) 2017, The State of the World's Children 2017: Children in a Digital World, UNICEF, ISBN 978-92-806-4930-7.