



Ministry of Information Technology, Communication and Innovation

Proposal to address the need for child online protection on social media

27 January 2025



The Need for Child Online Protection on Social Media

Preamble

In today's digital landscape, children are increasingly engaging with social media platforms, which offer avenues for learning, socialization, and entertainment. However, this heightened online presence also exposes them to significant risks, including exposure to inappropriate content, cyberbullying, and potential exploitation. Recent incidents in Mauritius have underscored the dangers of social networks that has an impact on the social, emotional and mental development, emphasizing the urgent need for effective child online protection measures. Recognizing these challenges, various efforts are being undertaken by the Ministry of Information Technology, Communication and Innovation in collaboration with the Ministry of Education and Human Resources and the Ministry of Gender Equality and Family Welfare to enhance safety protocols and restrict harmful content access to children. An effort has been made to establish comprehensive frameworks that will safeguard children's well-being in the digital environment, ensuring they can benefit from technological advancements without compromising their safety. An incident reporting portal known as the Mauritian Cybercrime Online Reporting System (MAUCORS+) has been also been established.

This proposal to protect children on social media is structured in the following manner.

The first section presents the executive summary. Section 2 defines the problem statement. Section 3 portrays the issues on social medias. Sections 4 talks about the Mauritian use case including the gravity of the problem. Section 5 put forward the measures and recommendations to address the social media challenges and finally the section 6 discusses the way forward.

¹MAUCORS+: <https://maucors.govmu.org>

² Educational video: <https://youtu.be/DXWPvJ6-PZY>

Table of Contents

1. Executive Summary	4
2. Problem statement.....	5
3. Background	5
4. Mauritian use case.....	8
5. Multipronged approach to be adopted	12
6. List of recommendations identified for the broader study.....	12
7. Proposed way forward	16

1. Executive Summary

Social media's widespread use has had a profound impact on how kids and teenagers communicate, learn, and interact with one another. Although these platforms have many advantages, they also put young users at risk, which emphasises how important it is to have strong child online safety measures. The social, emotional, psychological, and mental harm that children may sustain as a result of excessive social media use is a significant factor that needs to be properly assessed.

Children who spend too much time on social media run the risk of experiencing cyberbullying, inappropriate content exposure, negative effects on body image and self-esteem, sleep disturbances, social isolation, anxiety, decreased attention span, identity theft due to excessive sharing of personal information. In severe situations, they may also fall prey to revenge porn and sextortion. In Mauritius, in order to get an improved visibility on those risks, actions are being taken by the Computer Emergency Response Team of Mauritius (CERT-MU) to capture more granular data related to those risks through its Mauritian Cybercrime Online Reporting System (MAUCORS+). As of January 2024, Mauritius had approximately 820,900 social media users, accounting for 63.1% of the total population¹. Facebook remains the most popular social networking site in Mauritius, with around 58% of users being male, predominantly young students and professionals aged 14-24. A significant number of Mauritian adolescents have reported negative experiences, including exposure to inappropriate content and cyberbullying on social networks².

Suppressing objectionable online content, according to tech companies and free speech advocates, is against people's rights, including the right to free speech. Such arguments have frequently released large tech companies, especially social media platforms, from responsibility for damaging content. However, because such content poses both physical and emotional risks to children, governments and parents of children who have been harmed online, contend that these social media platforms should be regulated to safeguard and monitor children's access to it.

The degree of success that various nations have had in the past few years in tackling the issue of making the Internet safer for children varies. One important observation to be noted is that the common factor in legislations recently enacted in countries such as the UK, France, Canada, Australia and Germany is that the responsibility is being shifted onto online content providers such as social platform owners to regulate online harmful contents. Such an approach is possible only because these platforms have a point of presence in those countries, which is not the case for Mauritius.

In Mauritius, challenges are similar and therefore, a thorough study needs to be carried out in order to create a multifaceted framework that will allow kids to safely, responsibly, and confidently explore the digital world. This proposal identifies ten actions that should be examined in the comprehensive study. An Inter-Ministerial Committee will be setup to coordinate the formulation of an action plan that will be implemented by different stakeholders.

²

² <https://datareportal.com/reports/digital-2024-mauritius>

² <https://www.researchgate.net/publication/289588801>

2. Problem statement

A significant proportion of children worldwide are exposed to various online dangers. According to the Global Child Online Safety Index, 45% of online children across surveyed countries have experienced cyberbullying, 39% have faced reputational risks, and 29% have been exposed to violent and sexual content³. Another report “*A safer digital environment for children*” (March 2023), by the United Nations highlights that children and young people may encounter hate speech and violent content online, including messages that incite self-harm and even suicide⁴. Similarly, UNICEF emphasizes that children can be exposed to cyberbullying and other forms of peer-to-peer violence each time they log in to social media or instant messaging platforms⁵.

Digital harms can lead to a range of online, psychological, social, emotional and real-world issues, particularly among children and adolescents. Key impacts include aggressive behavior, hysteric state, distorted family life, lack of concentration, impaired memory and mental health issues.

This is an issue of concern and needs to be urgently addressed by the Government. Addressing this subject requires a multifaceted approach, including the implementation of robust online safety legislations and policies, the development of advanced technological safeguards, and the promotion of digital literacy among children, parents, and educators. Without immediate and concerted efforts to enhance child online protection, the negative impacts on children's mental health and well-being are likely to escalate, leading to long-term societal consequences. Therefore this proposal put forward the key measures and recommendations to tackle this problem.

3. Background

In recent years, there has been a significant increase in internet and social media usage among children and adolescents. A 2022 study by the Pew Research Center found that 95% of teens aged 13 to 17 have access to smartphones, and 97% use the internet daily, with 46% reporting they are online "almost constantly," a substantial rise from 24% in 2014-15. Social media platforms have become integral to youths' lives. YouTube is the most popular, with 95% of teens reporting usage. TikTok follows, used by 67% of teens, then Instagram at 62%, and Snapchat at 59%⁶. As of January 2024, there were approximately 820,900 social media users in Mauritius, representing about 63.1% of the total population.

The use of Internet and social network has created unprecedented opportunities for children and young people to communicate, connect, share, learn, access information and express their opinions on matters that affect their lives and their communities.

3

³ [https:// www.dqinstitute.org/news-post/](https://www.dqinstitute.org/news-post/)

⁴ <https://www.un.org/en/global-issues/child-and-youth-safety-online>

⁵ <https://www.unicef.org/protection/violence-against-children-online>

⁶ <https://www.pewresearch.org/>

However, access to the Internet and in particular, social media poses significant challenges to children's safety – both online and offline. To reduce the risks associated with these technologies while enabling more children and young people to reap its benefits, the Government along with its stakeholders has a critical role to play in establishing the foundations for safer and more secure use of Internet-based services and social media for today's children and future generations. In this endeavor, measures have to be taken by the Government to strengthen child online protection, including legislations and regulations.

Some of the Governments have worked in these lines and the case examples are as follows:

The United Kingdom (UK)

The United Kingdom has faced the challenges of controlling online harmful content for children and in October 2023, the British government passed the Online Safety Act to regulate harmful internet content, but it has drawn criticism for privacy infringement and its implementation is being rolled out slowly.

In mid-February 2024, ministers outlined new guidance for mobile phone and handset use for children, effectively barring their use during school hours. Concerned parents, however, were unsatisfied and continue to call for stronger internet safety measures. They fear that, after being forced away from their devices at school, kids will come home and immediately reach for their phones or devices. More pressing, the concern over exposure to both physical and emotional harm, including verbal and sexual abuse, bullying, etc. is insufficiently addressed by the current plan. This is the challenge, UK has to overcome.

Canada

Canada has the same problem as of UK where their children are exposed to harmful posts on social medias. The Canadian government has proposed a bill on February 26, 2024 called the Online Harms Act⁷, which would require social media platforms to remove harmful posts from their platforms within 24 hours. The legislation includes seven types of harmful content but makes a point of noting that the law will not impact private messages. The bill now needs to be studied by a parliamentary committee and the Senate, both of which may introduce changes before the draft is finalized. The challenge will be the implementation of the act because the Online Harms Act would apply to social media services, adult content services, and live streaming services.

France

France is also facing the issues related online child protection. In June 2023, the French government approved a new law that requires social media platforms to verify users' ages and obtain parental consent for anyone under 15 years old. The purpose of the law is to protect children from cyberbullying and other harmful effects of social media. However, according to

⁷ <https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c63.html>

Laurent Marcangeli, the law's main advocate in the French National Assembly, further advancements and regulations are necessary.

Similarly, members of the French National Assembly's Law Committee unanimously approved a bill that calls for protecting children's rights to their own images. The bill considers protecting a child's privacy to be among parents' legal duties. In February 2024, this Bill was enacted. This text marks a turning point by explicitly introducing children's image rights to the Civil Code, as part of provisions relating to parental authority. As the phenomenon of sharenting – the practice of sharing images of one's children on social networks – has intensified with the rise of digital technology, this legislation aims to regulate a practice that, while often perceived as harmless, can have serious consequences for minors' privacy.

Australia

Australia has a similar issue of child online protection. The country has passed the Online Child Safety Act in 2021, a comprehensive law that covers adult cyber abuse, image-based abuse, harmful content, cyberbullying, and more. Recently, Australian regulators updated the safety standards, which include requiring operators of cloud or messaging services to detect and remove child abuse and pro-terror material. At the same time, regulators are saying the new requirement will not compromise end-to-end encryption — if it does, they are sure to experience backlash from Apple and other messaging operators.

Moreover, in November 2024, an Online Safety Amendment (Social Media Minimum Age) Bill 2024 (the Bill) has been proposed. Its purpose is to amend the Online Safety Act 2021 to introduce an obligation on certain social media platforms to take reasonable steps to prevent children under 16 years of age from having an account. This Bill is still under discussion.

Germany

The situation in Germany with regards to the child online protection is not very different than other countries. Germany's Protection of Young Persons Act (JuSchG) regulates online safety for children and adolescents. The law was reformed in 2021 to address new online threats, such as cyberbullying and cyber-grooming. Under this Act, precautionary measures platforms must take steps to protect children from inappropriate content.

This includes:

- Child-friendly terms and conditions
- Safe default settings
- Easy-to-find information on reporting mechanisms

One important observation to be noted is that the common factor in the above legislations is that **the responsibility is being shifted onto online content providers such as social platform owners to regulate online harmful contents**. Such an approach is possible only because these platforms have a point of presence in those countries.

4. Mauritian use case

In Mauritius, the Cybersecurity & Cybercrime Act (CCA) 2021 already put burden on social media platform administrators to regulate online contents. The question is how effective is this provision in view of the absence of the social media representatives in the country. The CCA also has few provisions with respect to children online safety such as cyberbullying, revenge pornography and misuse of fake profile. However, there may still be a need for the Children’s Act 2020 and the CCA to be aligned. It is to be noted that the provisions such as Child Pornography, Child Grooming which are included in the Children’s Act may also need amendment.

With respect to resolution of incidents related to children on social media, the challenge is to have the presence of social media agencies locally. At once, Facebook appointed a moderator from the Mauritian Diaspora on request of the Government in 2022, but it was not effective in terms of timely content removal. Therefore, it is important to have this dialogue initiated again with Social Media Agencies to have their local representation in Mauritius.

Since the social media agencies do not have their offices in Mauritius, the other solution is to enact regulations for Internet Service Providers to prevent harmful content for children. For example, the ISPs can be mandated to provide free filtering tools with parental control where parents can set up content filters and establish time limits for Internet usage.

Another interesting data to consider is the statistics on incidents reported on the Mauritian Cybercrime Online Reporting System (MAUCORS+) from March 2018 to date. Although no stats for children specifically is available, it can be easily inferred that a large number of these complaints pertains to children and young adults given the typical profile of social media users in Mauritius and worldwide.

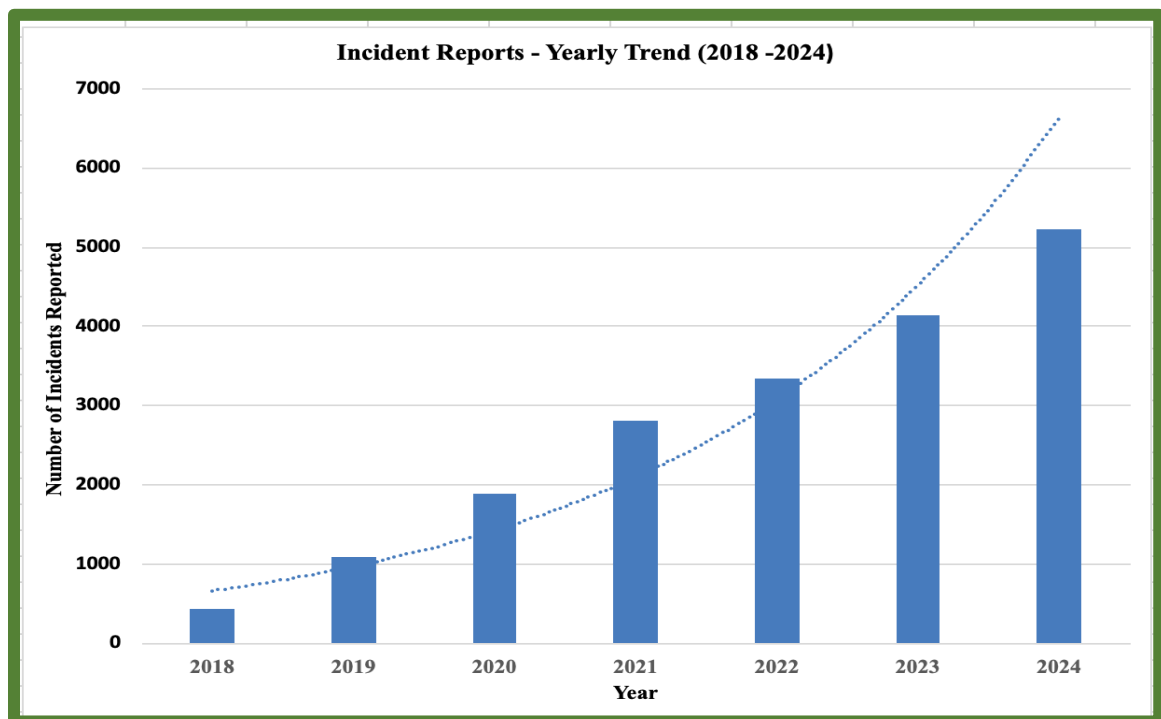


Figure 1: Yearly Incident Trend from 2018-2024 on MAUCORS+

Table 1: Incident Statistics (MAUCORS+)

Incident Type	No of Cases
Hacking	3840
Online Harassment	5465
Offensive Content	2361
Sextortion	652
Identity Theft	2023
Cyberbullying	1323
Cyberstalking	242
Scam and Fraud	3052
Phishing	167
Malware	63
Total	19188

The above figures reflect another parameter which justifies the urgent need for action in Mauritius.

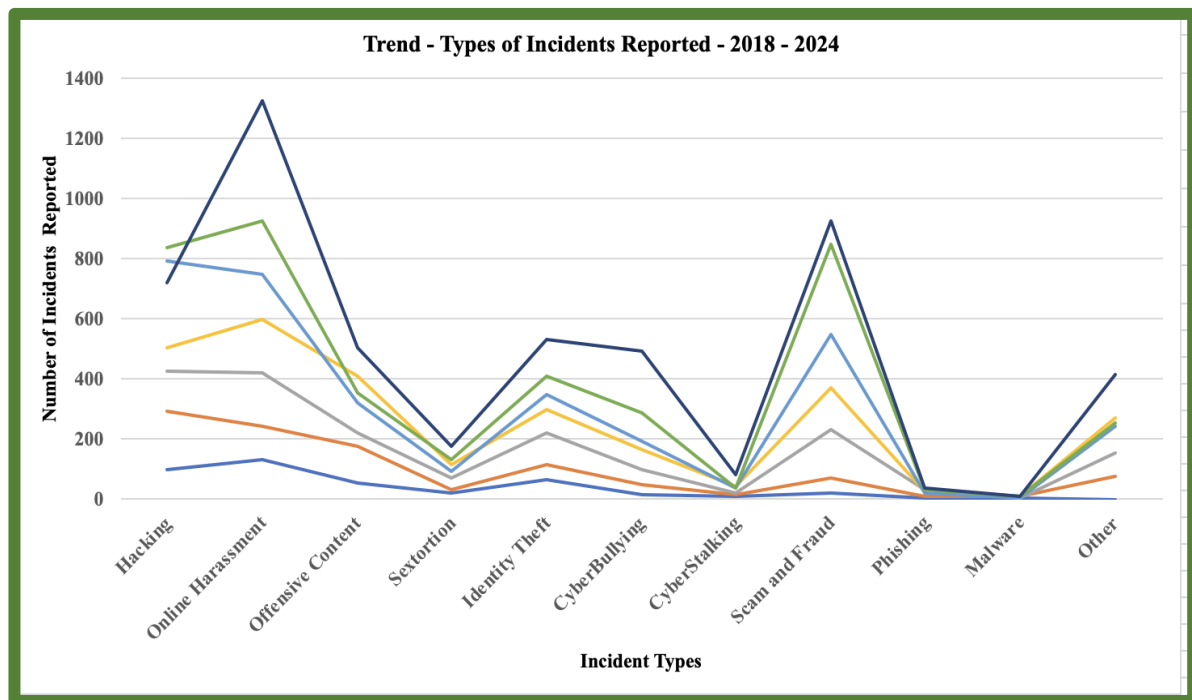


Figure 2: Types of Incidents Reported from 2018-2024 on MAUCORS+

A Glance at the Gravity of the Problem (Both local and International):

Therefore, to better understand the situation in Mauritius, NAFCO has conducted a survey on a group of young people aged 18 to 20. The findings of this survey are damning. More than 60% of female respondents have unwillingly received explicit content before 18 years old, and 97% of female respondents consider that pornography leads to 'pedo-pornography'. The comments left by respondents are utterly concerning and require immediate action. These have been quoted in the findings section.

Picture 1: Extract from NAFCO Mauritius Action Plan on the Online Safety of the Youth (January 2025)

• This article is more than 1 month old

Australia passes world-first law banning under-16s from social media despite safety concerns

Picture 2: News article from 'The Guardian' (28 November 2024)

As a child psychiatrist, I see what smartphones are doing to kids' mental health - and it's terrifying

Emily Sehmer



The online world is forcing children to grow up before they are ready, and parents need government's help to combat its harms

Picture 3: News article from 'The Guardian' (3 January 2025)

📷 'The longer you can put off children using smartphones, the better it is for them.' Photograph: Sally Anscombe/Getty Images

From stringent legislation to grassroots action, Australia and Spain lead the way in tackling children's use of mobile phones and tablets

Swipe le
... D'

Picture 4: News article from 'The Guardian' (11 January 2025)

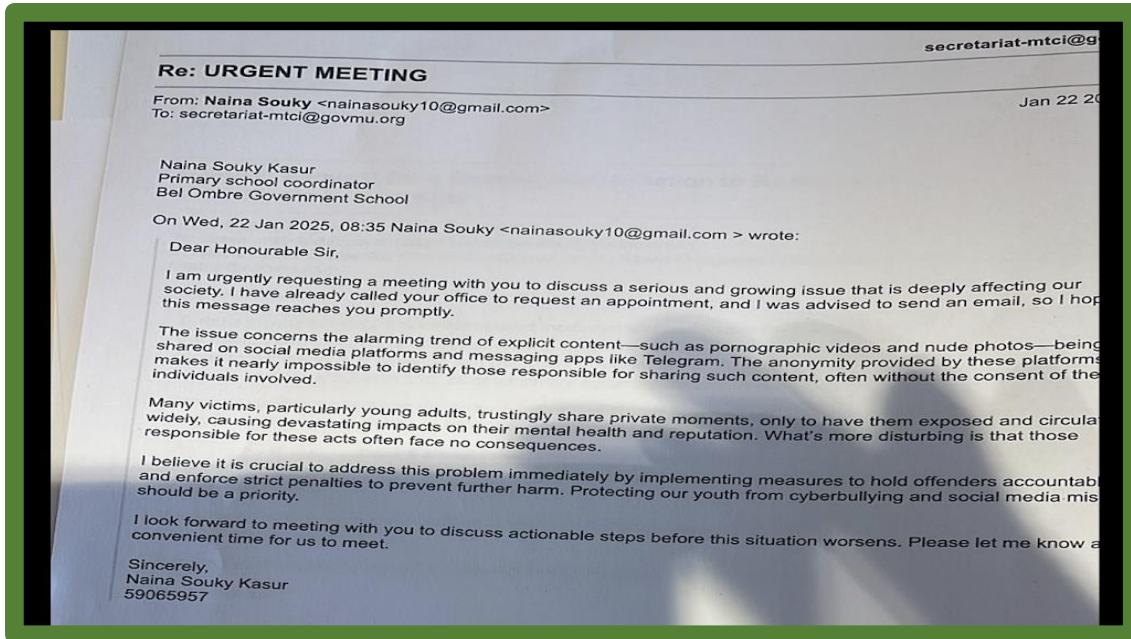
• This article is more than 1 month old

Explainer

How Australia's tough social media ban compares to laws in other countries

Laws will bar under-16s from accessing social media platforms such as Facebook, Instagram, Snapchat, Reddit and X

Picture 5: News article from 'The Guardian' (29 November 2024)



Picture 6: A copy of an email from Bel Ombre Government School sent to MTCI Secretariat related to explicit content (22 January 2025)

2.0 Telegram Scandal

Mauritius has been shocked by the scandal of telegram where NUDES of young girls (which include minors) and women were shared against their consent. This has created a tsunami wave of “revendication” about human rights, women rights, freedom and most importantly protection of human dignity.

Figures reported by the Mauritius Cybercrime Online Reporting System (MAUCORS) between 10th to 22nd March 2021, 148 cases have been reported – Cyberbullying , Cyberstalking, Sextortion, Cyber harassment etcⁱ. Research have proved that during lockdown period cases can rise up to three times and reported figures are just the tip of the iceberg of unreported cases. We acknowledge the rapid response taken by the cybercrime unit.

However, we are of opinion that we need to have a more holistic preparedness action plan with the rapidness of developing technologies.

Picture 7: Extract from Raise Brave Girls Proposal on Anti Cyberbullying Policies (March 2021)

5. Multipronged approach to be adopted

Bridging the gap on the legal front is only one work stream where action is needed. For example, the short, medium and long terms impact on Children’s social, emotional, development and the mental health is a major aspect which also need to be properly assessed. For instance, on social media, we may get a dopamine release from watching a funny cat video or reading a joke meme. Our brains want to continue this dopamine feedback loop, which can lead to mindless scrolling on Instagram or Facebook.

This is particularly challenging for children and can, in turn, lead to mental health issues. Students may become so hooked on scrolling through posts and chatting online that they lose track of time⁸. This habit can negatively impact their focus and study habits. Constant distractions from social media are a major reason for lower grades and reduced academic achievement. These two examples illustrate the plethora of issues which need to be addressed for a successful project implementation which produces tangible benefits to the society at large. In other words, there will be a need to commission a broader study for the development of a multipronged oriented framework aiming at creating a safer & more secure online environment for children by empowering them to explore the digital world safely, responsibly & with confidence.

6. List of recommendations identified for the broader study

I. Stocktaking exercise to strengthen the national legal framework

- Assess the need to update Mauritius’ Child Protection laws to specifically address online threats, bearing in mind the additional difficulties that we have in Mauritius regarding the lack of the point of presence of social media platforms in Mauritius. This could include:
 - Requiring online platforms, regardless of their physical presence, to comply with national standards for content moderation, privacy protection, and online safety for children (refer to figure 3 for ease of understanding).
 - Clear regulations that mandate social media platforms to remove harmful content (such as cyberbullying, hate speech, explicit content, or harmful challenges) within a specified timeframe.
 - Legal provisions for age verification to ensure that children do not access content meant for adults, including age-gated access to social media platforms.
 - Data Privacy and Security: Align with international standards like COPPA (Children’s Online Privacy Protection Act) to protect children’s data online, and ensure privacy laws prevent the misuse of personal data for children under 18.
 - Content Moderation Requirements: Establish minimum content moderation standards for platforms accessed in Mauritius, requiring them to implement automatic and manual systems for flagging and removing harmful content targeted at children.

4

⁴⁸ https://umu.divaportal.org/smash/get/diva2%3A1676381/FULLTEXT01.pdf?utm_source=chatgpt.com

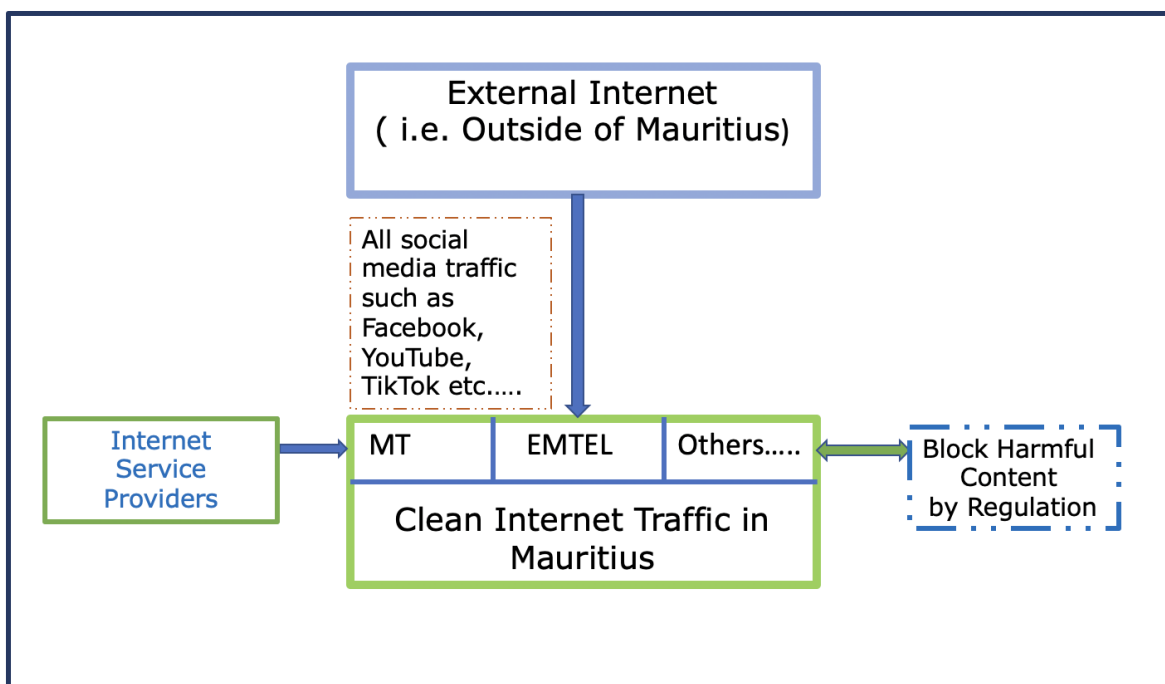


Figure 3: Concept of content moderation

II. *Explore the possibility for the creation of a National Child Protection Authority (COPA) for the Digital Space*

- responsible for overseeing child online safety issues, enforcing laws, monitoring the digital environment, and ensuring that platforms adhere to local regulations regarding child protection.
- which can collaborate with Global Entities: Since social media platforms operate internationally, COPA can collaborate with global organisations such as the Internet Watch Foundation (IWF), UNICEF, and regional child protection bodies to advocate for better practices and to facilitate international cooperation.

III. *Collaboration with International Platforms*

- Advocacy and lobbying for compliance: Even without a local presence, encourage global platforms (Facebook, Instagram, YouTube, etc.) to comply with Mauritius' child safety laws through advocacy and international pressure. This could include pressing these companies to:
 - Provide reporting channels accessible to children who are the victim of social media abuse (cyberbullying, cyber stalking, sexual exploitation, self-harm content).
 - Work with Mauritian authorities in content removal and response to online abuse or exploitation.
 - Support Mauritius' initiative by adopting local child protection policies, even without physical offices.

- Use International Frameworks: Encourage tech companies to adopt international standards such as the Global Internet Forum to Counter Terrorism (GIFCT) and the WePROTECT Global Alliance to prevent online exploitation of children.

IV. *Promote Digital Literacy and Education*

- Reinforce digital Literacy Programs for Children: Develop school-based and community-based programs to educate children about online risks and safe practices. Topics should include:
 - Recognising and reporting cyberbullying.
 - Protecting their privacy and understanding how to use privacy settings on social media platforms.
 - Understanding the risks of oversharing personal information and being aware of digital footprints.
 - How to spot harmful or inappropriate content (e.g., explicit material, scams, grooming behaviours).
- Parental Education and Awareness: Launch public awareness campaigns to educate parents and caregivers about the digital risks children face and the tools available to monitor and protect children’s online activity.
- Parental Control Tools: Provide guidance on setting up parental controls on popular social media platforms and devices (e.g., YouTube Kids, Facebook Family Center, Google SafeSearch, etc.).
- Provide resources and support for parents to help them communicate effectively with children about online dangers.

V. *Technology-Driven Solutions*

- Content Moderation Software and AI Tools: Advocate for or partner with local tech firms to develop and deploy AI-powered content moderation tools that can filter and block harmful content in real-time on platforms accessed by children. This could include:
 - Automatic filtering of explicit content (e.g., violent, sexually explicit, or bullying language).
 - Machine learning to detect and block harmful video or images (e.g., self-harm, child sexual abuse material).
 - Collaboration with ISPs: Work with Internet Service Providers (ISPs) in Mauritius to offer network-level content filtering that can block access to websites and platforms hosting inappropriate content for children.
 - Systems Age Verification: Advocate for stronger age verification protocols to restrict children from accessing platforms or content designed for adults. This could include multi-factor authentication and parental consent measures.

VI. *Enhance National Reporting Systems*

- National Helplines and Reporting Tools: Enhance the features of MAUCORS to categorise the incidents reported by children, parents, or educators and set up helplines. This system should allow:
 - Easy and confidential reporting of harmful content.
 - Integration with international hotlines and platforms like the National Center for Missing & Exploited Children (NCMEC).
- Cooperation with Platforms: Ensure that local authorities, even without a physical presence on the platform, can have effective means of reporting online harm, such as direct liaison channels with platform moderators or automated tools that alert local authorities when content is flagged.

VII. *Public-Private Partnerships and Stakeholder Collaboration*

- Collaboration with Private Sector: Engage social media companies, tech firms, ISPs, and telecom providers to be part of a national coalition for child safety. This collaboration should:
 - Foster joint initiatives to prevent online harm (e.g., joint campaigns on social media, co-developing educational resources for parents and children).
 - Encourage these companies to invest in safety technologies and provide financial support to local initiatives aimed at enhancing child protection online.
- NGOs and Civil Society Engagement: Partner with NGOs, child advocacy groups, and educational institutions to promote awareness, develop training programs, and create peer support networks for children and parents facing online challenges.

VIII. *Promote International Cooperation and Standards*

- Engage in Regional Child Protection Initiatives: Mauritius can engage in regional initiatives like the African Child Policy Forum or Southern African Development Community (SADC) to improve child safety measures across the region. These platforms can provide avenues for cross-border cooperation and sharing of best practices.
- Alignment with International Frameworks: Work with UNICEF, the Global Partnership to End Violence Against Children, and other international bodies to align with global child protection standards and to strengthen national policies that hold international platforms accountable.

IX. *Crisis Response and Victim Support*

- Crisis Management Framework: Develop a rapid response framework for cases of online child exploitation or abuse, ensuring swift legal action, support, and rehabilitation for victims.
- Support Services for Victims: Provide specialised services, including counselling and legal assistance, for children who experience online harm, such as cyberbullying, grooming, or exposure to distressing content.

X. *Monitoring, Evaluation, and Continuous Improvement*

- **Regular Assessments:** Conduct regular reviews and audits of the effectiveness of implemented measures, including the success of content moderation systems, public education efforts, and partnerships with international platforms.
- **Feedback Mechanisms:** Develop systems for ongoing feedback from children, parents, and educators to improve safety measures and adapt to emerging risks as digital technologies evolve.

7. **Proposed way forward**

Based on the above case examples and the different ways out, it is important to address the child online protection issues at the earliest. Therefore, the initiation of a broader study is a means to understand the ground realities and will facilitate to put in place the required legal, technical, organizational, capacity building and international collaboration measures.

Given the broad spectrum of issues to be tackled, it is important to get the buy-in of all relevant existing stakeholders in the Mauritian landscape. The starting point could be the setting up of an Inter-Ministerial Steering Committee to plan the implementation of the broader study which could be done in phases:

- **Phase I** – In depth study of the ten action lines recommended through the setting up different subcommittees consisting of both local and foreign resources specialised in the different themes therein
- **Phase II** – Review of the national legal framework by considering action lines 1,8 and 9 (in section VI)
- **Phase III** – Institutional review by considering action lines 3, 4, 8, 9 10 (in section VI)

The final outcome of the broader study will be to come up with the required action plan to be enforced by the different relevant stakeholders.

However, a quick win is to showcase Government's determination to address child online protection on social media. The proposal to envisage regulations for Internet Service Providers could be considered as a priority by the Inter-Ministerial Committee. In these regulations, the local Internet Service Providers could be mandated to provide free filtering tools with parental control where parents can set up content filters and establish time limits for Internet usage. For example, in Singapore, the Infocomm Media Development Authority (IMDA) has mandated certain measures, including providing parental control services, for online platforms and Internet Service Providers to help parents.