Andorra National Child Online Protection Assessment Report

Table of Contents

Acknowledgements

This report represents a collaborative effort between the International Telecommunication Union (ITU), the Government of Andorra, and key stakeholders across public, private, and non-governmental sectors. The report was developed by David Wright CBE, Director of UK Safer Internet Centre and Mr. Boris Radanovic Head of Engagement and Partnerships with support of Viktoriia Omelianenko, Project Officer, ITU Office for Europe and under supervision of Mr. Jaroslaw Ponder, Head of the ITU Office for Europe.

Special thanks are extended to H.E. Marc Rossell Soler, Secretary of State for Digital Transformation and Telecommunication, and David Vicente, Director of the National Digital Transformation Programme, for their leadership in advancing child online safety in Andorra. We also acknowledge the contributions of stakeholders from education, healthcare, telecommunications, and social services, whose perspectives shaped the findings and recommendations of this report.

Executive Summary

This report provides an in-depth assessment of child online safety in Andorra, offering a comprehensive overview of existing measures, challenges, and opportunities. Notably, this work benefits from a high level of political engagement with children's digital wellbeing, underscored by a mandate from the Head of State to prioritise this issue. Building on Andorra’s Digital Wellbeing Plan and aligned with ITU's Child Online Protection Guidelines for Policymakers, the report outlines a roadmap for strengthening the country's digital safety landscape.

Key recommendations include establishing a centralised Centre for Digital Wellbeing, enhancing public awareness, and developing forward-looking regulations to address both existing and emerging threats, with a particular emphasis on improving the protection offered to young people through the regulatory framework. Building on Andorra’s Digital Wellbeing Plan and aligned with ITU's Child Online Protection Guidelines for Policymakers, the report outlines a roadmap for strengthening the country's digital safety landscape. Key recommendations include establishing a centralised Centre for Digital Wellbeing, enhancing public awareness, and developing forward-looking regulations to address both existing and emerging threats.

1. Introduction

The rapid advancement of digital technologies has transformed the way children interact with the world, creating both opportunities and risks. In Europe these developments demand a comprehensive and adaptive approach to safeguarding young users. While digital connectivity enables educational access, social interaction, and skill development, it also exposes children to emerging risks, including AI-driven threats, harmful content exposure, cyberbullying, online exploitation, and data privacy challenges.

- *The Role of Artificial Intelligence in Child Online Safety*

Artificial intelligence (AI) is increasingly being used to enhance child online safety. AI-driven tools are capable of monitoring and detecting harmful content, identifying cyberbullying patterns, and flagging potential online grooming behaviours, enabling platforms and law enforcement to intervene more effectively. AI-powered content moderation is already being deployed across major digital platforms to identify and remove harmful material more efficiently than traditional human moderation. The European Union's AI Act underscores the importance of responsible AI deployment, introducing measures to ensure that AI applications interacting with children incorporate transparent safety mechanisms and ethical safeguards[1].

However, AI also introduces significant new risks. One major concern is the misuse of generative AI to create child sexual abuse material (CSAM). A recent report from the Internet Watch Foundation (IWF) found that AI-generated CSAM is growing at an alarming rate, with thousands of new images appearing on dark web forums. These AI-generated materials are becoming increasingly realistic and difficult to detect, presenting major challenges for law enforcement and content moderation efforts[2].

Similarly, the rise of AI-generated deepfake content presents serious risks to minors. In a recent case in Spain[3], schoolchildren created and distributed AI-generated explicit images of their classmates, leading to legal action and significant psychological harm. The increasing accessibility of AI-powered tools raises urgent concerns about misuse, digital ethics, and the protection of minors in online spaces.

- *Exposure to Harmful Content*

The risk of children encountering harmful and distressing content online remains a key concern. Social media platforms have faced scrutiny for their algorithm-driven promotion of harmful content, particularly relating to self-harm, eating disorders, and suicide. In a recent case in France, families filed lawsuits against TikTok, alleging that the platform's recommendation system pushed harmful content that directly contributed to tragic child suicides (AP News).

[1] AI regulation must keep up with protecting children - 5rights

[2] How AI is being abused to create child sexual abuse material (CSAM) online

[3] Spain sentences 15 schoolchildren over AI-generated naked images | Spain | The Guardian

Across Europe, research from the World Health Organization (WHO) Regional Office for Europe[4] has found a sharp rise in problematic social media use among adolescents, increasing from 7% in 2018 to 11% in 2022. Similarly, 12% of adolescents are at risk of problematic video gaming. These trends reinforce concerns about digital engagement patterns, highlighting the urgent need for digital literacy programmes to help children engage with online content safely and equip parents and educators with effective intervention tools.

- *Cyberbullying and Online Harassment*

Cyberbullying remains one of the most widespread and harmful digital risks for young people. Studies[5] indicate that one in four adolescents in Europe has experienced cyberbullying, leading to long-term psychological impacts, including anxiety, depression, and self-esteem issues.

Many cyberbullying incidents go unreported due to fear of retaliation or lack of trust in reporting mechanisms. AI is increasingly being integrated into cyberbullying detection systems, helping to identify harassment patterns in real time. However, such tools require responsible oversight, as AI systems alone cannot address the full complexity of peer-to-peer online interactions.

- *Sextortion and Online Exploitation*

The increase in sextortion cases, where children are coerced into sharing explicit images under threat, is a growing concern. Organised criminal networks exploit digital platforms to target young people, often resulting in severe psychological distress and, in extreme cases, suicide. Law enforcement agencies across Europe[6], including Europol and Interpol, have reported a sharp increase in sextortion cases, particularly targeting teenage boys.

AI is being used by criminal groups to create highly personalised scams, but it is also being deployed by law enforcement to track and disrupt exploitation networks. AI-powered behavioural analysis tools are already being trialled to identify and disrupt predatory online behaviours.

- *Manipulative and Addictive Design in Online Games*

Gaming platforms frequently employ manipulative design strategies, including loot boxes, in-game purchases, and variable reward systems, which encourage compulsive spending and excessive screen time among young players. These mechanics have been found[7] to mirror gambling behaviours, raising serious concerns over their impact on children's financial and mental well-being.

[4] Teens, screens and mental health

[5] Eurochild-Flagship-Report-Childrens-Realities-in-Europe.pdf

[6] NCA issues urgent warning about 'sextortion' - National Crime Agency

[7] [2207.09928] Upgrading the protection of children from manipulative and addictive strategies in online games: Legal and technical solutions beyond privacy regulation

Moreover, AI-driven personalised gaming algorithms are designed to maximise player engagement, making it harder for children to disengage. The WHO Europe study[8] found that 12% of adolescents are now at risk of gaming addiction, reinforcing the need for regulatory intervention, parental controls, and educational initiatives to promote healthy digital habits.

- *Privacy and Data Protection Concerns*

Children's personal data privacy is another major area of concern. Research[9] has shown that many child-focused digital platforms collect excessive amounts of data while failing to comply with strict data protection regulations. Non-compliance with EU General Data Protection Regulation (GDPR) protections has led to widespread exposure of children's personal data, increasing the risks of data breaches, identity theft, and targeted advertising.

AI-powered tracking and profiling further exacerbates these concerns, as platforms leverage behavioural data analysis to target children with personalised content, advertisements, and recommendations. Without strict privacy safeguards, children remain vulnerable to highly targeted and potentially harmful digital experiences.

To address these issues, the Government of Andorra partnered with the ITU to conduct a comprehensive assessment of the national landscape for child online safety. This report synthesises stakeholder consultations, global best practices, and existing frameworks to provide actionable insights and recommendations tailored to Andorra's unique context.

2. Digital Landscape Overview

Andorra's digital infrastructure ranks among the most advanced in Europe, providing nearly universal internet access and enabling a wide range of digital services. This robust connectivity has accelerated digital adoption across all age groups, including children, who are increasingly engaging with online platforms for education, recreation, and social interaction. However, recent studies, such as the UNICEF 2022 study on the impact of technology on teenagers in Andorra, show that 36.2% of teenagers engage in problematic internet use (PIU), with a higher prevalence among girls (41.3%) compared to boys (31.1%). Additionally, 14.3% of adolescents have experienced cyberbullying, and 20.1% of teenagers exhibit problematic video game use, with boys disproportionately affected at 28.3% compared to 10.9% of girls. These statistics underscore the urgent need to address digital risks specific to Andorra's youth, as problematic technology use is increasingly recognised as a public health concern.

The Andorra Digital Wellbeing Improvement Plan outlines a strategic framework to tackle these challenges by integrating digital wellbeing principles into public policies, ensuring a healthy balance between technology use and societal wellbeing. Emphasis is placed on fostering healthy digital habits, promoting screen time management, and equipping families with the tools to navigate the digital landscape responsibly.

[8] Teens, screens and mental health

[9] [2305.08492] On the conformance of Android applications with children's data protection regulations and safeguarding guidelines

3. Legal and Regulatory Framework

Analysis of the existing legal and regulatory framework revealed foundational measures for data protection and cybersecurity but identified gaps in addressing risks specific to children. International benchmarks, such as the UK's Online Safety Act and the EU's Digital Services Act, were highlighted as models for Andorra to emulate.

In developing a robust framework for child online protection, it is essential to consider key legislative aspects that have been effective in various jurisdictions. Aligning with the ITU COP Guidelines for Policy-makers[10], the following areas are pivotal:

1. Governance and Frameworks
   - Central Coordinating Body: Establish a dedicated agency to oversee digital safety, similar to Australia's eSafety Commissioner. This body would coordinate efforts across sectors to ensure a unified approach to online child safety.
   - Defined Roles and Responsibilities: Clearly delineate the duties of all stakeholders, fostering effective collaboration. Finland's model exemplifies successful multi-stakeholder engagement in this domain.
2. Legal Protections for Children Online
   - Criminalisation of Online Exploitation: Enact laws that criminalise activities such as grooming, sextortion, and the non-consensual distribution of images. The UK's Online Safety Act serves as a pertinent example.
   - Addressing Cyberbullying: Implement swift resolution mechanisms for cyberbullying incidents, inspired by New Zealand's Harmful Digital Communications Act.
   - Platform Accountability: Mandate that online platforms promptly remove harmful content, as demonstrated by Germany's Netzwerkdurchsetzungsgesetz (NetzDG).
3. Child-Centric Data Privacy
   - Stringent Data Protection Measures: Adopt comprehensive data protection regulations, akin to the General Data Protection Regulation (GDPR) in the European Union, emphasising parental consent and privacy by design.
4. Digital Literacy and Education
   - Mandatory Digital Literacy Education: Integrate digital literacy into school curricula and provide educators with training on online risks. Singapore and Norway offer successful models of such initiatives.

[10] Policy-makers | ITU-COP Guidelines

5. Technical Standards
    - Parental Controls and Content Filtering: Require the implementation of parental controls and content filtering mechanisms on devices, as practised in South Korea and France.
    - Social Network Safety and Age Verification: Establish regulations ensuring safety features and age verification processes on social networks to protect younger users.
6. Protections for Vulnerable Groups
    - Accessibility for Children with Disabilities: Ensure digital platforms are accessible to children with disabilities, following Canada's inclusive design standards.
    - Targeted Interventions for Marginalised Children: Develop specific strategies to support marginalised children, as seen in the Netherlands.
7. Reporting and Redress Mechanisms
    - Accessible Reporting Systems: Create confidential and user-friendly reporting systems for online harms, drawing inspiration from Australia's eSafety platform and the U.S. National Center for Missing & Exploited Children (NCMEC) reporting mechanism.

Emphasis was placed on implementing adaptable laws to address privacy challenges, such as encrypted communications. Regulatory parity with other countries, particularly neighbouring nations, was underscored to avoid the risk of Andorra having less stringent regulations, which could make it attractive to criminality, abusive behaviours, or other nefarious purposes. Moreover, there is much happening across the world with emerging and developing regulations, such as the Digital Services Act and Online Safety Act, which influence regional regulatory standards and highlight the need for Andorra to align with these global trends.

The ITU COP Guidelines for Policymakers provide a comprehensive framework to support the creation of a safe and empowering online environment for children. These guidelines recommend:

- Developing National Strategies: Formulate and implement national child online protection strategies that are inclusive and harmonised with international standards.
- Engaging Stakeholders: Involve all relevant stakeholders, including government entities, private sector, civil society, and children themselves, in the development and execution of these strategies.
- Continuous Evaluation: Regularly assess and update policies to address emerging risks and technological advancements.

By aligning Andorra's legislative framework with these guidelines and international best practices, the nation can strengthen its commitment to safeguarding children in the digital realm.

In addition to these global considerations, it was emphasised that an internal reflection is needed to identify specific areas that particularly affect Andorran society. This approach will ensure that proposed regulations are not only aligned with international best practices but also tailored to address the unique challenges faced within the principality.

Additionally, the Digital Wellbeing Improvement Plan proposes specific regulatory measures, such as the establishment of mandatory age verification procedures, the implementation of parental controls across all devices sold in Andorra, and the designation of the principle of 'minor by default' for websites using the .ad domain. These measures aim to create a safer digital environment for minors by ensuring platforms adhere to stringent child protection standards while empowering families with tools to monitor and regulate technology use.

4. Education and Public Awareness

Andorra's education system integrates digital safety into the curriculum, supported by a 12-step plan for promoting digital competencies in schools. This plan emphasises teacher training, device certification, and parental involvement. It is important to note that Andorra's educational landscape is composed of three coexisting systems, and the plan discussed in the session applies specifically to the Andorran system.

The Digital Wellbeing Improvement Plan adds further clarity by emphasising the integration of digital skills education at every grade level, fostering security and privacy awareness, and equipping students with problem-solving skills for navigating digital environments. The plan includes the creation of high-quality, age-appropriate digital learning content and the training of educators to identify and address risks like online addiction and digital violence. Furthermore, stakeholders highlighted the need to consider the protection of children during extracurricular activities. Training professionals involved in these activities to detect problematic digital behaviours was also identified as a key priority.

Awareness campaigns tailored to cultural and socioeconomic contexts, such as Safer Internet Day[11], were identified as effective strategies to enhance public education efforts. These campaigns should incorporate interactive tools and resources for families, including workshops, digital literacy assessments, and the promotion of family technology contracts to establish healthy usage norms at home.

5. Youth Engagement

Engaging youth as active participants in online safety initiatives was a key theme. Young people are among the most active users of digital platforms, and their perspectives provide essential insights into emerging online risks, platform behaviours, and the effectiveness of safety interventions. Studies[12] indicate that when young people are meaningfully involved in

[11] SID Homepage

[12] Digital technologies policy brief.pdf

shaping digital policies, the resulting frameworks are more likely to be relevant, sustainable, and aligned with their real-world experiences.

To facilitate meaningful engagement, structured participation mechanisms should be embedded in child online safety initiatives. These may include:

1. Youth Advisory Councils: Establishing formalised youth advisory groups, such as those used in the EU's Better Internet for Kids initiative[13], ensures that young people have a direct channel to provide feedback on digital policies and child safety measures.

2. Peer-to-Peer Education: Studies highlight that young people are more likely to absorb and respond positively to online safety messages when they come from their peers. In Finland, initiatives like the Mannerheim League for Child Welfare's youth digital mentors programme[14] have successfully empowered students to lead safe internet campaigns and support digital well-being discussions in schools.

3. Anonymous Feedback Channels: Many young people hesitate to report online harms due to concerns about stigma or retaliation. Platforms and policymakers should implement confidential reporting mechanisms, ensuring young users can express their concerns safely. The EU Youth Dialogue[15] provides a model for capturing youth opinions and translating them into actionable policy recommendations.

4. Gamification and Digital Engagement: Interactive digital literacy initiatives, such as AI-driven chatbots, gamified learning tools, and real-world scenario simulations, have proven effective in engaging youth in online safety education. Denmark's CyberPilot project[16] integrates gaming elements into cybersecurity training for young people, demonstrating higher engagement and retention of safety knowledge.

Overcoming mistrust between youth and adults was identified as a key challenge, with participants advocating for visible action based on youth input. Studies suggest that when youth contributions lead to clear policy outcomes—such as changes in platform safety tools or educational initiatives—trust and engagement increase significantly[17]. Establishing transparent feedback loops where young people see the impact of their participation is essential to maintaining trust and long-term engagement in child online safety efforts.

6. Technical Tools and Support Channels

Discussions highlighted the need for enhancing technical tools, such as parental controls and SIM-based restrictions, to protect children online. Andorra Telecom provides several key safety features, including filtered internet services designed to block harmful content and ensure safer browsing experiences. Additionally, Andorra Telecom offers parental control

[13] Home | Better Internet for Kids

[14] Front page - The Mannerheim League for Child Welfare

[15] European Youth Portal | European Youth Portale

[16] CyberPilot | Awareness training & Phishing training

[17] OECD Digital Education Outlook 2023 | OECD

options, allowing parents to set usage limits, monitor activities, and customise access to specific types of content.

The Digital Wellbeing Improvement Plan supports these efforts with actionable proposals, such as distributing routers pre-configured with child-safe Wi-Fi networks, implementing a SIM card mode with carrier-side blocks for inappropriate content, and publishing detailed guidelines for configuring parental controls across various devices. Additionally, plans for a physical support office for parental control setup aim to provide hands-on assistance to families. These initiatives are complemented by proposals to block inappropriate content on public Wi-Fi networks and explore potential regulations on minors' access to public internet services. Challenges related to emerging privacy standards, such as encrypted traffic, were also addressed, emphasising the importance of balancing safety and privacy.

7. Stakeholder Engagement

The importance of multi-sector collaboration was emphasised, with calls for creating a governance board to coordinate child online protection efforts. Existing models, such as Safer Internet Centres in France and Spain, were highlighted as examples of effective stakeholder engagement.

Effective reporting and support systems must be accessible, trusted, and designed with input from young users. Research indicates that many young people do not report online harms due to a lack of trust in reporting mechanisms, fear of consequences, or uncertainty about available support[18].

To ensure reporting systems meet the needs of children and young people, the following mechanisms should be considered:

- Youth-Informed Platform Design – Consultation with young people on how reporting tools should function leads to higher engagement and effectiveness. In the UK, the Child Exploitation and Online Protection (CEOP) Centre worked with young people to redesign their online reporting tool, significantly increasing its use among teenagers[19].
- Confidential and Anonymous Reporting Options – Young people are more likely to report online risks if they feel protected from retaliation. The EU Youth Dialogue has shown that anonymous digital reporting tools increase the likelihood of incident reporting[20].
- Youth-Led Awareness on Reporting – Many young people are unaware of reporting mechanisms or do not know how to use them. The Australian eSafety Commissioner has engaged youth as digital safety ambassadors, helping to raise awareness among their peers about when and how to report online harms[21].

[18] European Youth Portal | European Youth Portal

[19] Report to CEOP

[20] European Youth Portal | European Youth Portal

[21] YRRC Research Report eSafety 2021_web V06 - publishing_1.pdf

Ensuring that young people are actively involved in shaping and promoting reporting mechanisms will improve trust in these systems and increase their use, ultimately strengthening Andorra's overall approach to child online protection.

Regular cross-sectoral workshops and international partnerships were recommended to maintain progress and adapt to emerging threats.

8. Establishment of the Digital Skills and Wellbeing Agency (BCD Agency)

The proposed BCD Agency was outlined as a central entity for managing child online protection initiatives. Drawing inspiration from similar agencies in Australia and New Zealand, its roles and responsibilities include coordination, monitoring, and fostering innovation. Recommendations emphasised the need for clear operational guidelines and partnerships with international organisations to ensure success.

The establishment of the BCD Agency was identified as a critical step in ensuring a coordinated, evidence-based approach to child online safety in Andorra. Stakeholder discussions highlighted several gaps in governance, implementation, and monitoring, reinforcing the necessity of a dedicated agency to lead national efforts in digital wellbeing.

Anticipated impact of the BCD Agency

1. Bridging the Coordination Gap – While various government bodies, private entities, and civil society groups are involved in digital wellbeing efforts, there is no single entity responsible for overseeing child online protection. The ITU COP Guidelines[22] stress the importance of centralised governance mechanisms to ensure alignment between regulations, education, law enforcement, and industry standards. The BCD Agency will unify and streamline these efforts to maximise impact and efficiency.
2. Addressing Andorra's Specific Digital Risks – The Andorra Digital Wellbeing Improvement Plan identified key online risks, including problematic internet use, cyberbullying, online exploitation, and lack of digital literacy resources for parents and educators. The BCD Agency would:
    - Lead national digital wellbeing campaigns tailored to Andorra's unique challenges.
    - Develop policy interventions to mitigate the risks associated with excessive screen time, online grooming, and misinformation.
    - Implement and monitor safety regulations, ensuring compliance with international child protection standards.
3. Strengthening Public Awareness and Digital Literacy – The ITU COP Guidelines highlight the need for comprehensive awareness programmes and digital literacy initiatives to empower families, educators, and children. The BCD Agency will:

[22] Policy-makers | ITU-COP Guidelines

- Coordinate digital literacy training for schools, ensuring that educators, students, and parents receive targeted guidance on online risks, safe internet use, and responsible digital citizenship.
- Facilitate youth engagement initiatives, such as peer-led awareness programmes and youth digital safety councils, which have been successfully implemented in Finland and Denmark.
- Ensure accessibility of resources, leveraging multilingual and age-appropriate content to reach diverse segments of the population.

4. Improving Law Enforcement and Reporting Mechanisms – The stakeholder consultation identified a lack of user-friendly, confidential reporting systems for children experiencing online harm. The BCD Agency will:
    - Develop and promote national reporting platforms, similar to Australia's eSafety reporting tool and the UK's CEOP system, allowing children and families to report online harms easily and securely.
    - Work with law enforcement to enhance capacity-building for online child protection investigations and strengthen cross-border cooperation to combat online exploitation.
    - Ensure tech industry accountability, advocating for stronger content moderation policies in line with the EU's Digital Services Act.
5. International Alignment and Global Partnerships – ITU and stakeholders emphasised the importance of international collaboration to enhance Andorra's approach to child online safety. The BCD Agency will:
    - Engage with international partners, including ITU, the UK Safer Internet Centre, and the European Commission, to exchange best practices and secure technical support.
    - Participate in global child online protection initiatives, ensuring that Andorra remains aligned with evolving international standards and regulatory frameworks.
    - Contribute to international research, leveraging Andorra's small-scale but digitally advanced infrastructure as a testbed for innovative digital safety solutions.
6. The establishment of the BCD Agency is a positive step in ensuring a sustainable, proactive, and internationally aligned approach to child online protection in Andorra. By centralising governance, coordinating public education efforts, strengthening enforcement mechanisms, and leveraging international partnerships, the agency will play a transformative role in safeguarding young people's digital wellbeing.

9. Prioritised Recommendations and Implementation Plan

To guide action and ensure impact, the following recommendations are prioritised based on urgency, feasibility, and anticipated impact:

1. Establish the BCD Agency

- **Implementation Approach:** Define the agency's roles and responsibilities to encompass coordination, monitoring, and fostering innovation. Develop operational guidelines to ensure accountability and transparency. Build partnerships with international organisations such as ITU to leverage expertise and resources.
- **Success Metrics:** Operational establishment within one year, engagement of key stakeholders, and demonstrable coordination of at least three national initiatives.

2. Develop a Comprehensive Regulatory Framework

- **Implementation Approach:** Align regulations with international best practices, including age verification and content moderation. Address emerging challenges such as encrypted communications and ensure adaptability for technological advancements.
- **Success Metrics:** Enactment of new regulations within 18 months, measurable reduction in access to harmful content, and compliance by major technology providers.

3. Expand Teacher Training and Certification

- **Implementation Approach:** Design and deliver training programmes for educators to address risks such as online grooming and harmful content. Certify school devices to meet digital safety standards and create clear protocols for online safety incidents.
- **Success Metrics:** Training of 80% of educators within two years and certification of all school devices.

4. Launch Tailored Public Awareness Campaigns

- **Implementation Approach:** Collaborate with community leaders, influencers, and media to design segmented campaigns addressing cultural and socioeconomic diversity. Focus on educating parents, children, and educators through accessible resources.
- **Success Metrics:** Execution of campaigns across all municipalities, increased use of parental control tools by 50%, and positive feedback from families.

5. Enhance Technical Tools and Support Channels

- **Implementation Approach:** Improve usability of parental control tools and develop innovative solutions such as New Zealand's "unboxing" project. Address privacy challenges through coordinated measures with ISPs.
- **Success Metrics:** Adoption of improved tools by 60% of families and successful pilot of innovative projects.

6. Foster Governance and Stakeholder Collaboration

- **Implementation Approach:** Establish a governance board to oversee child online protection initiatives. Organise regular workshops to align stakeholders and share best practices. Partner with international organisations to secure funding and expertise.
- **Success Metrics:** Formation of the governance board within six months, regular quarterly workshops, and measurable progress in international collaboration.

7. Develop Baseline Indicators for Digital Wellbeing

- **Implementation Approach:** Define and implement key indicators to assess the degree of children's digital wellbeing in the country. These indicators should measure areas such as online safety, mental health impacts of technology use, and the effectiveness of implemented initiatives.
- **Success Metrics:** Establishment of a baseline within one year, regular publication of digital wellbeing reports, and measurable improvements in identified key areas over time.

Conclusion

By prioritising these key recommendations and implementing them effectively, Andorra can establish a robust framework for child online safety. Continued stakeholder engagement, rigorous evaluation, and alignment with global best practices will ensure sustainable progress in safeguarding children in digital environments.

Annex: Detailed Agenda and Comprehensive Discussion Points

Child Online Protection Assessment Stakeholder Consultation

2nd December 2024, Andorra la Vella

9:00-10:00 Introduction

The introductory session emphasised the importance of collaborative efforts in advancing child online safety. ITU experts presented key resources, including guidelines and capacity-building activities, tailored to address Andorra's unique needs. Stakeholders highlighted the critical role of inclusive policies and shared a commitment to actionable solutions.

10:00 - 10:30 Digital Wellbeing and Protection for Children

Stakeholders discussed the current state of children's digital engagement in Andorra, focusing on screen addiction, cyberbullying, and the vulnerabilities children face in digital spaces.

Recommendations:

- Conduct a comprehensive national assessment of children's digital engagement.
- Promote family agreements and involve parents in digital safety practices.
- Integrate the six principles of digital well-being—access and participation, privacy, protection, training and awareness, family responsibility, and social implications—into policy frameworks.

10:30 - 11:30 Legal and Regulatory Framework

Participants examined Andorra's legal landscape, noting gaps in enforcement mechanisms and adaptability to emerging threats such as encryption.

Recommendations:

- Develop enforceable regulations aligned with international best practices, including age verification and content moderation.
- Explore adaptable frameworks to accommodate technological advancements, referencing models from South Korea and Bermuda.
- Balance privacy considerations with child protection needs.

11:45 - 12:45 Education Initiatives

Stakeholders praised the 12-step plan for promoting digital competence but stressed the importance of comprehensive teacher training and resources.

Recommendations:

- Expand teacher training to address online grooming, harmful content, and emerging digital risks.
- Certify school devices to ensure they meet safety standards.
- Engage parents through workshops and accessible resources.

13:45 - 14:30 Public Education and Awareness

Public education campaigns were identified as key to fostering safe online habits. Examples such as France’s segmented campaigns and Croatia’s intergenerational approach were discussed.

Recommendations:

- Tailor awareness campaigns to diverse audiences based on cultural and socioeconomic contexts.
- Collaborate with influencers and community leaders to enhance campaign reach.
- Develop multi-layered initiatives addressing the specific needs of parents, children, and educators.

14:30 - 15:15 Youth Engagement

Participants emphasised the importance of youth participation in shaping policies and programs.

Recommendations:

- Establish youth councils to provide ongoing feedback and insights.
- Implement anonymous feedback channels to capture candid perspectives.
- Build trust between youth and adults through consistent, actionable engagement.

15:15 - 16:00 Technical Tools and Support Channels

Stakeholders evaluated existing tools like parental controls and discussed innovative approaches to device management.

Recommendations:

- Enhance the usability of parental controls and ensure clear guidance for parents.
- Adopt innovative projects like New Zealand’s “unboxing” initiative to improve device safety.
- Address privacy challenges posed by encrypted traffic through coordinated safety measures.

16:00 - 16:45 Stakeholder Engagement

The session highlighted the need for a governance framework to coordinate multi-sector efforts.

Recommendations:

- Create a governance board to oversee child online protection initiatives.
- Organise regular cross-sectoral workshops to align stakeholders and share best practices.
- Foster international partnerships with organisations like ITU for capacity building and funding.

16:45 - 17:45 Establishment of the BCD Agency

The BCD Agency’s structure was outlined, drawing from successful international models.

Recommendations:

- Define the agency’s roles clearly, focusing on coordination, monitoring, and innovation.
- Build international partnerships to leverage expertise and resources.
- Establish operational guidelines to ensure accountability and transparency.

17:45 - 18:00 Conclusions and Next Steps

The consultation concluded with a commitment to advancing the outlined recommendations. Immediate priorities include establishing the BCD Agency and aligning Andorra’s regulatory framework with global standards. Continuous stakeholder engagement and robust evaluation mechanisms were emphasised as critical for success.