ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY

Research Report

CHILDREN'S ONLINE PRIVACY, SAFETY, AND WELL-BEING IN KOSOVO

March 2026

CHILDREN'S ONLINE PRIVACY, SAFETY, AND WELL-BEING IN KOSOVO

Current Landscape, Stakeholder Findings, Implications, and Recommendations

Institute for Technology and Society (ITS)
Prishtina, 2026

CHILDREN'S ONLINE PRIVACY, SAFETY, AND WELL-BEING IN KOSOVO

Current Landscape, Stakeholder Findings, Implications, and Recommendations

Publisher: Institute for Technology and Society (ITS)

Prishtina, March 2026

This research was carried out as part of the HumanRightivism project, funded by the Swedish Embassy in Prishtina and implemented by the Community Development Fund (CDF). The views expressed in this research are those of the Institute for Research and Human Rights and do not necessarily reflect the views of the donor.

Contents

Executive Summary

This report examines children's online privacy, safety, and well-being in Kosovo through a policy-oriented lens that combines stakeholder-based evidence with international and local sources. Prepared within the **"Privacy First"** project, it explores how parents, teachers, and school actors understand and respond to online risks affecting children, and situates these issues at the intersection of digital rights, child protection, education, and mental well-being. The report argues that online safety should be understood not only as a technical matter, but also as a social, relational, and institutional one.

The report draws on evidence generated through **one workshop and three training sessions** implemented with parents, teachers, school staff, psychologists, and institutional representatives. In total, **80 participants** were reflected in the evaluation. Baseline and post-session tools were used to assess participants' perceptions of online risks, confidence in responding to incidents, and the immediate value of the activities.

The findings point to a clear pattern. Participants did not begin from a position of indifference; they already regarded children's online risks as serious and relevant. At baseline, the most frequently identified concerns included **cyberbullying (52.5%)**, **harmful or inappropriate content (46.2%)**, **oversharing of personal data (46.2%)**, and **excessive screen use with implications for well-being (38.8%)**. However, this awareness was not matched by practical readiness. Confidence in taking protective steps emerged as the weakest baseline area, with **57.5%** of respondents placing themselves at the lower end of the scale and none reporting very high confidence.

Post-training results indicate meaningful immediate gains in understanding and orientation. Participants reported improved understanding of children's digital privacy, clearer awareness of the roles of parents and teachers, and better recognition of the links between online risks and children's well-being. The sessions were also widely assessed as useful, relevant, and understandable. At the same time, the evidence suggests that short-format interventions alone cannot fully address deeper practical and institutional gaps. Participants continued to express the need for follow-up support, practical examples, clearer response protocols, and stronger coordination between schools and families.

Taken together, the report supports three main conclusions. First, children's online privacy and safety in Kosovo should be treated as **social, educational, and child protection issues**, not only as questions of digital literacy. Second, the main gap identified through the project is not a lack of concern, but a lack of **practical readiness, procedural clarity, and confidence** among adult stakeholders. Third, while targeted trainings can improve awareness and orientation, stronger long-term impact will require continued capacity-building, clearer institutional pathways, and more consistent cooperation between parents, schools, and relevant public actors.

Against this background, the report concludes that improving children's online privacy and safety in Kosovo requires a more coordinated and practice-oriented response. This includes strengthening communication and trust between adults and children, improving school-level response and referral pathways, and ensuring that online safety is integrated into broader child protection and well-being efforts rather than treated as a stand-alone technical issue.

1. Introduction and Methodology

1.1 Introduction

Children's everyday lives are now deeply shaped by digital environments. Communication, learning, entertainment, peer interaction, and self-expression increasingly take place through smartphones, social media platforms, messaging applications, and online content ecosystems. This shift has created new opportunities for connection and access to information, but it has also expanded the range of risks children face in relation to privacy, safety, dignity, and emotional well-being. Across Europe, research has consistently shown that children's online experiences include not only opportunities, but also exposure to cyberbullying, harmful content, unwanted contact, misuse of personal information, and other forms of digital vulnerability.[1][2]

These issues matter not only because children may encounter inappropriate or harmful situations online, but because the effects often extend beyond the digital sphere. Online humiliation, unwanted sharing of images or personal information, peer harassment, exclusion, and manipulative contact can affect a child's sense of security, trust, confidence, sleep, concentration, and willingness to seek help. International evidence increasingly points to the importance of understanding children's online experiences not only through the lens of technology, but also through the lenses of mental health, peer dynamics, child protection, and adult support systems. [3]

In Kosovo, these concerns are especially relevant in a context where children's digital access is high, institutional support structures are still developing unevenly, and practical guidance for parents and teachers remains limited. UNICEF Kosovo has highlighted cyberbullying and online safety as pressing concerns and notes that internet access among young people is widespread, while national and local systems are still in the process of developing stronger protective responses. The need for grounded, context-specific analysis is therefore not merely academic; it is directly connected to how families, schools, and institutions can better protect children while respecting their rights and dignity.

This report was developed within that context. It forms part of the project "Privacy First: Empowering Parents and Teachers to Protect Children's Mental Health in the Digital Age," which was designed to raise awareness, strengthen adult capacity, and produce practical resources on children's online privacy and safety. The approved project concept framed the problem as one of growing online risks, insufficient digital literacy among adults, and the danger that surveillance-heavy or dismissive reactions may undermine trust and unintentionally cause harm.[4]

The report does not seek to provide a definitive national measurement of children's online experiences in Kosovo. Rather, it aims to offer a structured and evidence-informed account of the current landscape, combining project-based findings with international and local literature. In doing so, it treats children's online privacy and safety not only as a technical issue, but as a social, educational, and protection issue that requires informed adult engagement, stronger coordination, and practical responses.

---

[1] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey Results from 19 Countries. London School of Economics and Political Science. Available at: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

[2] World Health Organization Regional Office for Europe. (2024, March 27). One in six school-aged children experiences cyberbullying, finds new WHO/Europe study. Available at: https://www.who.int/europe/news-room/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study

[3] UNICEF Kosovo Programme. (2024). Think before you share. Available at: https://www.unicef.org/kosovoprogramme/think-you-share

[4] Institute for Technology and Society, *Baseline and Post-Training Findings: Workshop and Training Sessions on Children's Online Privacy and Safety* (2026).

1.2 Purpose of the Report

The purpose of this report is fourfold. First, it seeks to provide a concise but analytically grounded overview of the current landscape of children's online privacy, safety, and well-being, with particular attention to the kinds of risks, dilemmas, and support needs that affect parents, teachers, and schools. Second, it presents the findings generated through one stakeholder workshop and three training sessions conducted under the project, using pre- and post-session questionnaires and facilitator observations as the primary empirical basis.

Third, the report interprets these findings in light of international and local evidence. This includes major European and global research on children's online experiences, cyberbullying, and adolescent well-being, as well as Kosovo-relevant sources on online safety, child protection, and institutional response. Fourth, it develops practical and policy-relevant recommendations aimed at parents, teachers, schools, and relevant institutional actors.

The report is therefore positioned between a project report and a policy paper. It is grounded in the realities of project implementation, but it also aims to contribute to broader discussion on how Kosovo can better address the intersection of children's rights, digital safety, privacy, and emotional well-being.

1.3 Research Questions

This report is guided by the following questions:

- What are the main online privacy and safety risks affecting children and adolescents, as reflected in international evidence and Kosovo-relevant sources?
- How do parents, teachers, and other school-related actors understand and respond to these risks in practice?
- What gaps exist in knowledge, confidence, communication, coordination, and institutional preparedness?
- What do the findings from the workshop and training sessions reveal about stakeholder needs, priorities, and perceived capacity?
- What practical and institutional recommendations emerge from the evidence?

1.4 Scope and Limitations

The report is based on a defined and intentionally limited evidence base. Its primary empirical material comes from one workshop and three training sessions, supported by a baseline questionnaire and a final evaluation form. In total, the underlying analytical exercise covered 80 participants, including teachers, parents or guardians, school management and staff, and a small number of education directorate or institutional representatives.

This means that the report should not be read as a statistically representative study of all parents, teachers, or children in Kosovo. Its value lies instead in identifying recurring patterns and concerns among directly engaged stakeholders, examining the practical readiness of adult actors who play a central role in children's digital environments, and linking these findings to broader evidence and policy-relevant recommendations.

The report also does not attempt to make clinical conclusions about children's mental health, nor does it claim to prove causal relationships between specific digital practices and psychological outcomes. Where international literature discusses associations between social media use, online harms, anxiety, sleep disruption, or reduced well-being, such evidence is used carefully and interpretively rather than deterministically.

1.5 Methodology

1.5.1 Overall Approach

The report adopts a small-scale, applied research approach that combines primary project-based evidence with secondary desk research. The objective was not to generate abstract or purely theoretical discussion, but to build an evidence base that could inform practical guidance, training priorities, and broader reflection on the state of children's online privacy and safety in Kosovo.

This approach brought together three layers of evidence. The first consisted of data generated directly through project activities: a stakeholder workshop, three adult-focused training sessions, and accompanying baseline and post-session questionnaires. The second consisted of facilitator observations and interpretive notes generated during implementation. The third consisted of desk research drawing on international and Kosovo-relevant sources, including institutional reports, guidance documents, and selected academic or analytical literature.

1.5.2 Primary Data Sources

The core empirical basis of the report comes from the project's implemented activities. According to the internal evaluation summary, the activity format consisted of one workshop and three training sessions, with 80 participants reflected in the analysis. The instruments used were a baseline questionnaire and a final evaluation form, designed to capture both participants' starting point and their assessment of the sessions after completion.

The baseline questionnaire focused on participant profile, initial knowledge, perceptions of current risks and conditions, confidence in responding to incidents, existing practices, institutional and practical gaps, and priority support needs. The final evaluation form focused on perceived learning, usefulness, relevance, role clarity, practical confidence, and demand for continued support.

The participant profile was mixed and appropriate to the topic. Teachers formed the largest group, followed by parents or guardians, school management and other staff, and a small number of institutional participants. This composition is analytically important because it brings together actors who experience the issue from different vantage points: parents observe children in everyday home settings, while teachers and school staff encounter issues in structured educational environments and are more likely to think in terms of procedures, referrals, and institutional roles.

1.5.3 Secondary Data Sources

To avoid reading the project findings in isolation, the report draws on a targeted body of international and local literature. Internationally, it relies on established sources concerning children's online risks, cyberbullying, adolescent well-being, and digital habits, including European and global evidence from EU Kids Online, WHO/HBSC, and UNICEF.

At the Kosovo level, the report uses available institutional and programmatic materials relevant to online safety, child protection, school response, and awareness-raising. These include UNICEF Kosovo materials and Kosovo's child protection and referral framework, which help situate the stakeholder findings in the broader local policy and implementation context.

Selected interpretive literature is also used where helpful to explain broader dynamics, particularly around constant connectivity, social comparison, sleep, emotional strain, and the developmental pressures associated with digital life. Such sources are used cautiously and in dialogue with institutional evidence rather than as stand-alone authority.

1.5.4 Data Analysis

The analysis combines descriptive and thematic methods. The questionnaire data is read descriptively, using frequencies, percentages, and mean scores to identify broad patterns in participant

responses. This includes participants' baseline knowledge, confidence levels, perceptions of risk, and post-session assessments of usefulness, clarity, and self-reported learning.

Alongside this, open-ended responses and workshop or training observations are interpreted thematically. Particular attention is given to recurring concerns around communication, trust, incident response, school–family coordination, practical knowledge gaps, and demand for clearer institutional procedures. The report does not treat project data and literature as separate silos. Instead, it uses a light form of triangulation: project findings are read against broader evidence, and broader evidence is used to contextualize local stakeholder perceptions without overstating what the project data alone can prove.

1.5.5 Ethical Note and Methodological Adaptation

The report is based on anonymous and aggregated activity data. The questionnaires used for the workshop and trainings did not require detailed personal identification, and findings are reported at group level. Any illustrative statements drawn from open responses or activity discussions should therefore be presented in anonymized form and, where appropriate, attributed only by general role category rather than by name or institution.

It is also important to note that the original project design anticipated a broader qualitative research phase involving interviews and focus groups. During implementation, however, the research component was operationalized through a more proportionate and practice-oriented structure centered on stakeholder engagement through one workshop, three trainings, and structured questionnaires. This does not invalidate the report; rather, it situates it more clearly as an applied policy and practice paper based on stakeholder engagement, training-linked evidence, and desk research.

2. Conceptual and Analytical Framework and International Landscape

This section situates the report within a broader conceptual and international evidence base. It clarifies how children's online privacy and safety should be understood, outlines the main categories of digital risk identified in international literature, and examines how these risks relate to trust, social pressure, reporting barriers, and emotional well-being. It also introduces selected interpretive perspectives, including the debate around constant connectivity and the 'phone-based childhood', while maintaining a cautious distinction between association and causation.

2.1 Conceptual and Analytical Framework

2.1.1 Understanding children's online privacy and safety

Children's online privacy and safety should not be understood narrowly as technical matters concerning passwords, privacy settings, or device use. In practice, privacy includes children's control over personal information, images, conversations, location data, online identity, and the conditions under which information about them is shared, stored, or circulated. Safety, by contrast, concerns protection from harm: this includes harassment, coercion, manipulation, humiliation, fraud, exploitative contact, and exposure to content or interactions that undermine dignity or well-being. These dimensions overlap. A child whose images are shared without consent, for example, faces both a privacy breach and a safety risk, especially when the material becomes a tool of humiliation, exclusion, or blackmail.

This broader understanding is consistent with international research that treats children's online experiences as part of a wider ecology of rights, opportunities, and vulnerabilities. The EU Kids Online framework, for example, distinguishes among content risks, contact risks, conduct risks, and contractual or commercial risks, while also emphasizing that online environments are not inherently harmful or inherently empowering. Their effects depend on context, age, digital skills, support structures, and the nature of the child's social environment.[5]

2.1.2 Why digital risks are social, relational, and educational

A central premise of this report is that digital risk is rarely only digital. Many of the harms that concern parents and schools begin online but are produced through social relationships. Cyberbullying, for instance, is not simply a communication problem on a platform; it is rooted in peer dynamics, status competition, exclusion, and the visibility that digital environments give to humiliation. Likewise, unwanted contact from strangers becomes dangerous not only because of the technology through which it occurs, but because children may lack the confidence, support, or language to disclose it early.

This means that privacy and safety should also be approached as educational and relational questions. Family communication patterns, teacher responses, peer norms, trust in adults, and school reporting culture all shape whether risks escalate or are addressed in time. International evidence suggests that children are more likely to seek help when they believe adults will respond calmly, take them seriously, and avoid blame or overreaction. By contrast, punitive or alarmist responses may discourage disclosure even when children recognize that something is wrong.[6]

2.1.3 Children's online experiences and well-being

The relationship between digital life and well-being has become one of the most debated issues in contemporary child policy. It is now widely accepted that some online harms, especially

[5] Danah Smahel et al., *EU Kids Online 2020: Survey Results from 19 Countries* (London: London School of Economics and Political Science, 2020), available at: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf.

[6] Smahel et al., *EU Kids Online 2020*; UNICEF Europe and Central Asia Regional Office, *Ending Violence against Children in Europe and Central Asia: Focus on Online Risks, Cyberbullying, and Protection* (2024).

cyberbullying, coercive contact, humiliation, and exclusion, can affect children's sense of security, belonging, and emotional stability. What remains debated is the strength and nature of the relationship between broader digital exposure particularly social media and smartphone use and mental health outcomes such as anxiety, low mood, reduced attention, or sleep disruption.

For policy and practice purposes, two points are important. First, the absence of a simple causal formula does not mean the concerns are overstated. Many children experience online pressures that are plainly distressing, even if those effects vary by context and cannot be reduced to one variable. Second, well-being impacts often operate indirectly: through social comparison, public visibility, peer pressure, sleep displacement, or the feeling of being permanently reachable. These pathways are especially relevant when children lack stable adult support or when the online and offline environments around them reinforce each other negatively. [7]

2.1.4 Interpretive perspectives and current debates

Recent public debate has been strongly shaped by arguments that describe a shift from a 'play-based childhood' to a 'phone-based childhood', in which smartphones and social media expose children to constant comparison, fragmented attention, sleep disruption, and reduced in-person interaction. Jonathan Haidt's The Anxious Generation has become one of the most visible contributions to this debate. The book is useful in policy discussions because it synthesizes a wide range of concerns in accessible terms and highlights mechanisms particularly social comparison, chronic connectivity, and sleep loss that are frequently echoed in schools and families.[8]

At the same time, the academic literature cautions against overstating causal certainty. Several scholars have argued that the relationship between digital technology and adolescent mental health is real but complex, with effect sizes that vary across outcomes and populations. Nature summarized this tension by describing the evidence base as important but far from settled, especially when broad claims are made about smartphones or social media as singular causes of deteriorating well-being.[9] For this reason, this report uses The Anxious Generation as an interpretive lens rather than as a definitive authority. Its value lies in helping explain patterns that may emerge in stakeholder data, not in replacing institutional and peer-reviewed evidence.

2.2 International Landscape

2.2.1 Common categories of online risk

International evidence consistently points to several recurring categories of digital risk for children and adolescents. First, children encounter content risks, including violent, sexualized, hateful, or otherwise harmful material. Second, they face contact risks, such as unwanted approaches from strangers, grooming, or manipulative communication. Third, conduct risks arise from interactions with peers, including cyberbullying, exclusion, rumor spreading, non-consensual sharing of images, and coordinated humiliation. Fourth, privacy and commercial risks involve data extraction, public exposure of personal information, scams, manipulative design, and commercial profiling. [10]

---

[7] World Health Organization Regional Office for Europe, "One in Six School-Aged Children Experiences Cyberbullying, Finds New HBSC Study," March 27, 2024, available at: https://www.who.int/europe/news-room/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study; Amy Orben and Andrew K. Przybylski, "The Association between Adolescent Well-Being and Digital Technology Use," *Nature Human Behaviour* 3

[8] World Health Organization Regional Office for Europe, "One in Six School-Aged Children Experiences Cyberbullying, Finds New HBSC Study," March 27, 2024, available at: https://www.who.int/europe/news-room/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study; Amy Orben and Andrew K. Przybylski, "The Association between Adolescent Well-Being and Digital Technology Use," *Nature Human Behaviour* 3

[9] "The Evidence on Social Media and Adolescent Mental Health Remains Contested," *Nature* 627 (2024): 466–467.

[10] Smahel et al., *EU Kids Online 2020*.

These categories often overlap in practice. A child who shares a photo under peer pressure may later face humiliation, coercion, or wider circulation of personal material. Similarly, an account security failure can quickly become a conduct risk if unauthorized access is used to impersonate the child or publish embarrassing content. The practical relevance of these overlaps is important for prevention: adults often underestimate how quickly a seemingly minor privacy lapse can turn into a more serious safeguarding issue.

2.2.2 Digital access, exposure, and age-related vulnerability

Children's exposure to online risk must be interpreted in the context of widespread device access and everyday connectivity. Across Europe and in neighboring contexts, smartphones have become the dominant point of access to online life, while social media and messaging applications increasingly shape peer relationships, identity formation, and leisure. EU Kids Online found that online engagement begins early and intensifies with age, while digital skills do not always keep pace with digital exposure. In other words, increased use does not automatically mean increased resilience.[11]

Age remains a major factor. Younger children may be less able to identify manipulation, understand privacy implications, or interpret misleading content, while adolescents often face stronger peer pressure, image-based social comparison, and reputational risks. This does not mean older children are necessarily less vulnerable. Rather, the nature of vulnerability changes: risks become more closely tied to identity, social standing, intimate communication, and the pressure to remain continuously visible and responsive.

2.2.3 Cyberbullying, humiliation, and reporting barriers

Among the most consistently documented risks is cyberbullying. The latest HBSC findings published by WHO Regional Office for Europe reported that around one in six school-aged children in the region had experienced cyberbullying, underlining the extent to which digital aggression has become embedded in adolescent life.[12] What distinguishes cyberbullying from many offline harms is not only the hostility itself, but also the persistence, visibility, and potential scale of the audience. Harmful content can circulate quickly, remain searchable or shareable, and reappear over time.

Reporting remains a major challenge. International research indicates that children do not always disclose online harm even when they recognize it as distressing. They may fear embarrassment, punishment, disbelief, further exposure, or restrictions on device use. This makes adult response quality critically important. Children are more likely to disclose when they expect calm, practical, and non-judgmental support. This insight is central to the present report because it links privacy and safety directly to communication practices within families and schools.

2.2.4 Constant connectivity, sleep, and emotional strain

A growing body of literature has examined how constant connectivity can intensify emotional strain even outside clearly identifiable incidents such as bullying or grooming. Scholars and policy commentators have drawn attention to the role of late-night device use, pressure to respond quickly, exposure to idealized images, and the sense that social life is always happening elsewhere and in real time. These mechanisms are frequently associated with sleep disruption, reduced concentration, emotional exhaustion, and increased vulnerability to anxiety or low mood. [13]

Yet the literature also warns against simplistic narratives. Not every child who uses social media heavily will experience poor mental health, and digital technology can also support belonging,

[11] Smahel et al., *EU Kids Online 2020*.
[12] World Health Organization Regional Office for Europe, "One in Six School-Aged Children Experiences Cyberbullying, Finds New HBSC Study."
[13] Haidt, The Anxious Generation; World Health Organization Regional Office for Europe, "One in Six School-Aged Children Experiences Cyberbullying, Finds New HBSC Study."

information access, creativity, and social connection. The policy challenge, therefore, is not to frame digital life as uniformly harmful, but to identify the conditions under which it becomes harmful and the forms of support that reduce risk. This is one reason why the present report emphasizes mediation, trust, and practical readiness rather than simply screen-time reduction as an end in itself.

2.2.5 Protective factors and lessons from international evidence

Across the literature, several protective factors recur. First, children benefit from supportive and communicative relationships with adults who take online concerns seriously without defaulting to blame or panic. Second, digital skills matter, but they are most effective when paired with judgment, emotional support, and realistic guidance. Third, schools play an important role not only through formal procedures, but through climate: children are more likely to report harm where norms are clear, adult responses are consistent, and peer cruelty is not minimized. Fourth, institutional clarity matters. Even modest protocols and referral paths can reduce uncertainty and prevent the diffusion of responsibility.[14]

These lessons are highly relevant for Kosovo and for the findings presented later in this report. They suggest that effective responses should not focus only on digital restrictions or technical awareness campaigns. They should also strengthen communication, normalize help-seeking, clarify responsibilities, and provide adults with practical ways to recognize, document, and respond to online harm. This is precisely where stakeholder-based evidence from workshops and trainings becomes valuable: it helps identify whether these protective factors are present, weak, or unevenly understood in the local context.

[14] Smahel et al., *EU Kids Online 2020*; UNICEF Europe and Central Asia Regional Office, *Ending Violence against Children in Europe and Central Asia* (2024); World Health Organization Regional Office for Europe, "One in Six School-Aged Children Experiences Cyberbullying, Finds New HBSC Study."

3. Kosovo Context

Any assessment of children's online privacy, safety, and wellbeing in Kosovo must be read against two parallel developments. On the one hand, children and adolescents are growing up in a digital environment in which smartphones, messaging platforms, video content, and social media are part of everyday communication, entertainment, and learning. On the other hand, the institutional and practical systems meant to support children in these spaces remain uneven, often depending on the initiative of individual schools, parents, teachers, or partner organisations rather than on fully consolidated routines. For that reason, the Kosovo context is not defined only by access to technology, but by a wider question of preparedness: how families, schools, and institutions understand online risks, how they respond to incidents, and how clearly responsibilities are distributed.

3.1 Digital Context in Kosovo

Kosovo is a highly connected society in demographic terms, with children and young people using digital tools and online platforms from an early age. Recent Kosovo-focused evidence and programme material suggest that smartphones are the dominant access point for internet use among children and adolescents, and that online engagement extends well beyond formal educational purposes.[15] This matters because the online environment is no longer a secondary space; it is woven into friendship, identity, entertainment, peer validation, and information consumption. As a result, the boundary between online and offline harm is often thin, especially when humiliating or threatening experiences circulate quickly through peer networks.

The practical significance of this digital exposure is reflected in the kinds of concerns that local actors increasingly identify: cyberbullying, unwanted sharing of photos or information, peer pressure in digital spaces, exposure to harmful content, account security problems, and unsafe contact from strangers. These are not abstract risks. They affect whether a child feels safe in school, whether they continue to participate confidently in peer life, and whether they are willing to disclose a problem to a trusted adult. In Kosovo, as elsewhere, the expansion of digital access has therefore increased the need for adult guidance that is both informed and proportionate.

3.2 Institutional and Policy Context

The institutional picture in Kosovo shows that children's online safety is recognised as a legitimate concern, but the level of operational readiness varies. At policy and programme level, ministries, municipalities, schools, child-protection actors, and independent institutions all have a relevant role.[16] In education settings, schools and municipal education directorates are often the first point of contact when a problem becomes visible. In more serious situations, child-protection and referral structures become relevant, particularly where risks affect a child's safety, dignity, or emotional wellbeing.

In recent years, awareness-raising and guidance efforts have become more visible.[17] UNICEF Kosovo and its partners have publicly emphasised the importance of safer online behaviour, including through campaigns aimed at cyberbullying prevention and support for child-focused online safety work.[18] The Ministry of Education, Science, Technology and Innovation has also supported practical

[15] UNICEF Kosovo Programme, *Think Before You Share* (2024), available at: https://www.unicef.org/kosovoprogramme/think-you-share; UNICEF Kosovo, "Closing Gaps for Children in Kosovo: EU and UNICEF Drive Systemic Change to Protect the Most Vulnerable," 2025.
[16] Assembly of the Republic of Kosovo, *Regulation No. 18/2024 on the Referral Mechanism and Protocol for Institutional Responsibility Regarding Child Protection* (2024); Ministry of Education, Science, Technology and Innovation, *Navigating the Internet* (2024).
[17] UNICEF Kosovo Programme, *Think Before You Share*; Ministry of Education, Science, Technology and Innovation, *Navigating the Internet* (2024); UNICEF Kosovo, "Closing Gaps for Children in Kosovo," 2025.
[18] UNICEF Kosovo Programme, *Think Before You Share*; UNICEF Kosovo, "Closing Gaps for Children in Kosovo," 2025.

guidance material on safer internet use. These developments are important because they show that the issue is no longer peripheral. At the same time, the existence of guidance does not automatically mean that all schools or families have the same level of clarity on what to do when an incident occurs, how to document it, when to escalate it, or how to communicate with children in a way that encourages disclosure rather than silence.

Kosovo's broader child-protection framework also matters for this discussion. The applicable referral and reporting rules provide an important normative basis for institutional response where a child may be at risk. Yet, in practice, the challenge is often less about the complete absence of formal rules and more about translation into everyday use. Teachers may not always be certain whether an incident should be treated as a disciplinary issue, a safeguarding issue, or both. Parents may be unsure whether to approach the school first, a psychologist, a municipal authority, or the police. This uncertainty can delay response and increase the burden on children.

3.3 Local Evidence and Observed Gaps

Compared with broader international evidence, Kosovo still has a relatively limited public evidence base specifically focused on children's online privacy and safety. There are useful institutional and programmatic materials, and some local studies touching on cyberbullying, digital behaviour, and child wellbeing, but the field remains fragmented. This creates a familiar gap: the issue is widely acknowledged, yet practical knowledge remains uneven and frontline actors often rely on intuition rather than consistent procedures.

Several recurring gaps appear across available local material and project experience. First, awareness does not always translate into action. Many adults recognise that children face online risks, but they are less confident when it comes to concrete response steps. Second, school-family coordination can be inconsistent. Even where both parents and teachers are concerned, they may not share the same understanding of supervision, boundaries, privacy, or reporting responsibilities. Third, support structures are not always visible to children themselves. If a child does not know whom to trust, or expects blame rather than support, a formal mechanism may exist without being meaningfully accessible. [19]

A further challenge lies in the practical character of the issue. Online privacy and safety problems are often dynamic, emotionally charged, and shaped by peer cultures that move faster than formal institutions. A humiliating image or message can spread quickly, and its consequences may be felt immediately at school. In these situations, adults do not only need general awareness; they need judgement, communication skills, and a shared understanding of how to respond in ways that protect the child without escalating harm.

3.4 Why a Practical Stakeholder-Based Assessment Matters

This context helps explain why a stakeholder-based assessment is valuable in Kosovo. Where the public evidence base is still developing and school realities differ, project-based engagement with teachers, parents, school representatives, psychologists, and education officials can generate insight that is both grounded and usable. It does not replace large-scale research, but it can reveal how the issue is actually understood in practice: what adults worry about most, where confidence is low, what kinds of support they consider realistic, and which forms of intervention are most likely to be adopted.

[19] Danah Smahel et al., *EU Kids Online 2020: Survey Results from 19 Countries* (London: London School of Economics and Political Science, 2020); UNICEF Europe and Central Asia Regional Office, *Ending Violence against Children in Europe and Central Asia* (2024).

The value of this approach is especially clear in a field where imported recommendations do not always fit the local context. Kosovo does not need a purely abstract conversation on children's digital risks. It needs responses that are practical, school-aware, and realistic for families and institutions working with limited time and resources. A report rooted in stakeholder engagement is therefore useful not only as a descriptive exercise, but as a bridge between international evidence and locally relevant action.

4. Findings from the Workshop and Training Sessions

This section presents the empirical findings generated through the workshop and three adult training sessions implemented under the project. Rather than reproducing the monitoring summary mechanically, it interprets the results in light of the broader analytical framework developed in the preceding sections. The findings are therefore read as evidence of how parents, teachers, school staff, and institutional actors currently understand children's online privacy and safety, where they feel least prepared, and what kinds of support they regard as most useful in practice.

4.1 Overview of Activities and Participants

The findings in this chapter draw on one stakeholder workshop and three training sessions delivered to adult participants, supported by a baseline questionnaire and a final evaluation form. In total, 80 participants are reflected in the analytical summary used for this report. The participant profile was mixed but not evenly distributed, with teachers forming the largest group, followed by parents or guardians, school management and other staff, and a smaller number of education directorate or institutional representatives.[20]

Respondent category	n	Share (%)
Teachers	30	37.5
Parents/guardians	28	35.0
School management and other staff	20	25.0
Education directorate / institutional staff	2	2.5

This composition matters analytically. Teachers and school staff are more likely to encounter digital safety concerns in a structured educational setting, often in relation to reporting, classroom dynamics, and safeguarding responsibilities. Parents and guardians, by contrast, may observe children's everyday behaviour more closely but feel less certain about institutional procedures, escalation pathways, or school-based coordination. Taken together, the participant mix offers a useful window into the adult support environment surrounding children's digital lives in the targeted school communities (ITS, 2026a).

4.2 Baseline Findings

The baseline results point to a pattern that is consistent with the report's wider argument: concern about children's online risks already exists, but practical readiness is much weaker. Participants did not enter the sessions indifferent to the issue. On the contrary, they broadly recognised that children face meaningful privacy and safety risks online. What appeared less developed was the ability to identify these risks consistently, respond to them in a structured way, and rely on clear institutional routines when incidents occur.

4.2.1 Initial knowledge and awareness

Across the baseline knowledge items, the starting point can be described as uneven and generally low to moderate. Participants showed some recognition of the importance of digital privacy and of the connection between online experiences and children's well-being, but more practical dimensions such as identifying risks systematically or taking concrete protective steps started from a

[20] Institute for Technology and Society, *Baseline and Post-Training Findings: Workshop and Training Sessions on Children's Online Privacy and Safety* (2026).

weaker position. This suggests that the issue was already perceived as important, yet not sufficiently understood in operational terms.

4.2.2 Recognition of risk and limited confidence to act

One of the clearest baseline messages concerns confidence. Participants tended to recognise that children face significant online risks, but many were unsure what to do when confronted with a concrete incident. Very high confidence was absent altogether, while the largest shares clustered in the lower-confidence categories. The pattern is important because it shows that awareness of risk does not automatically translate into response capacity. In practice, adults may know that a problem is serious without being sure how to intervene, whom to inform, or what immediate steps to prioritise (ITS, 2026a).

Confidence level	n	%
Very confident	0	0.0
Somewhat confident	9	11.2
Neutral	12	15.0
Somewhat not confident	32	40.0
Not confident	27	33.8

Read together with the baseline questionnaire structure, this low-confidence pattern indicates that participants' main need was not simply more general awareness but more concrete guidance: how to recognise incidents early, how to respond proportionately, how to communicate with children, and how to navigate responsibilities between home and school.

4.2.3 Current practices, institutional gaps, and support priorities

The baseline responses also suggest that some protective practices were already in use. These included general rules at home or in school, informal monitoring, and basic conversations about safe behaviour. Yet more structured or institutionalised measures appeared much weaker. The least consolidated areas included formal reporting mechanisms, clear school procedures, consistent guidance on privacy settings, and dependable coordination between parents and schools. Participants also pointed repeatedly to broader constraints: lack of practical knowledge, unclear institutional processes, children's reluctance to disclose problems, and the rapid evolution of digital platforms.

When asked what kind of support they needed, participants did not primarily ask for abstract information. Their answers clustered around a narrower and more practical set of priorities: incident handling, communication with children, privacy settings and digital hygiene, school procedures, and reporting pathways. This point is significant for the report as a whole. It indicates that adults do not only need sensitisation; they need usable frameworks that fit their actual roles and responsibilities.

4.3 Post-Training Findings

The post-session evaluation presents a clearly positive picture, although one that still requires cautious interpretation. Participants reported that the sessions were useful, relevant to their roles, and generally clear and understandable. The strongest gains appear in understanding and role clarity, while improvements in practical confidence are meaningful but somewhat more moderate. This is a plausible pattern for short-format training interventions, where immediate learning often precedes deeper behavioural change.

Post-session item	Mean score	Rated 4–5 (%)	Rated 1–2 (%)
Improved understanding of children's digital privacy	4.4	87.5	2.5

Greater confidence in taking practical protection steps	4.2	76.2	3.8
Better understanding of effects on well-being and support needs	4.3	82.5	2.5
Clearer understanding of parental and teacher roles	4.4	86.2	1.2
Session was useful and relevant	4.6	92.5	0.0
Content was clear and understandable	4.5	90.0	1.2
Practical component was sufficient	4.1	73.8	3.8
Session length was appropriate	4.2	77.5	2.5

4.3.1 Immediate learning and role clarity

The first four post-session items are especially revealing. Participants reported stronger understanding of digital privacy, better appreciation of the effects of online experiences on children's well-being, and much clearer understanding of the roles of parents and teachers. In a project that explicitly aimed to move adults away from either dismissive or overly intrusive responses, these gains are significant. They suggest that the sessions succeeded in reframing the issue from a narrow technical concern into a broader matter of supportive, privacy-respecting adult engagement.

4.3.2 Practical confidence and applicability

Self-reported confidence in taking practical protection steps also improved, although the ratings are slightly less emphatic than those related to understanding and relevance. This is a realistic result. It suggests that participants left the sessions with better orientation and stronger readiness, but not necessarily with the sense that every practical challenge had been resolved. The internal evaluation summary likewise notes that the most realistic interpretation is not full transformation, but meaningful movement from general concern toward more structured understanding and improved immediate readiness.

The post-session responses further indicate that participants did not perceive the sessions as abstract. They connected the content to concrete situations in homes, classrooms, and school-community communication. This matters in a topic area where adults often need both judgement and practical steps. The findings therefore support the idea that the training design particularly the use of realistic examples and role-based discussion was broadly appropriate to the needs identified at baseline.

4.3.3 Continued demand for support

Despite the positive assessment, the sessions were not experienced as sufficient in themselves. Participants continued to ask for more training, practical tools, concrete incident scenarios, clearer institutional protocols, and user-friendly guidance materials. Rather than indicating dissatisfaction, this pattern appears to show that the sessions helped participants articulate their needs more precisely. After the intervention, demand did not disappear; it became more structured and more specific.

4.4 Thematic Interpretation of the Findings

- **Concern is high, but readiness is lower.** Across the baseline responses, participants already perceived children's online risks as significant. The main deficit was not whether adults cared, but whether they felt equipped to respond effectively. This distinction is analytically important because it suggests that awareness-raising alone is insufficient; adults need pathways for action.
- **Communication and trust remain central.** Although technical issues such as passwords, account security, and privacy settings mattered, the findings repeatedly pointed toward relational concerns: whether children would report problems, whether adults would respond proportionately, and whether the response would protect rather than undermine trust. This aligns closely with the

project's original premise that over-controlling or dismissive adult behaviour can itself create harm when children face online risks.

- **Institutional consistency is weaker than informal action.** Many respondents appear to rely on informal rules, monitoring, or ad hoc conversations, while more formal mechanisms school procedures, reporting pathways, clearer division of roles, and coordination between actors remain less developed. In this sense, the findings are not only about individual knowledge gaps, but about institutional fragility.
- **Participants value practical, role-based guidance.** The strongest post-session scores concern usefulness, clarity, and role relevance. At the same time, the continued call for examples, case handling, and protocols indicates that participants want support that is practical, scenario-based, and immediately applicable.
- **The issue is understood as both technical and social.** The findings do not support a narrow cybersecurity-only interpretation. Participants gave considerable weight to communication, well-being, peer pressure, reporting, and coordination. This reinforces the report's broader argument that children's online privacy and safety should be treated as a behavioural, educational, and child-protection issue as much as a digital-literacy issue.

4.5 Findings in Light of the Literature

When read alongside the international and Kosovo-oriented literature discussed in earlier sections, the workshop and training findings appear both credible and unsurprising. European research has long shown that children's online environments are shaped not only by exposure to technical risks but also by peer dynamics, social pressure, reporting barriers, and the quality of adult mediation. Studies across Europe consistently suggest that supportive communication, confidence in reporting, and coherent school responses are among the most important protective factors. [21]

The project findings mirror that pattern closely. Participants did not place all emphasis on devices or settings; they repeatedly returned to communication, trust, uncertainty about response steps, and the need for clearer institutional pathways. This is also broadly consistent with Kosovo-relevant materials that point to the need for stronger awareness, practical guidance, and more coherent child protection and referral responses in school and community settings.

The findings therefore do not stand apart from the literature; they give it local texture. They show how broader international concerns translate into the practical realities of schools and families in Kosovo, and they provide a grounded basis for the implications and recommendations developed in the next section.

[21] Danah Smahel et al., *EU Kids Online 2020: Survey Results from 19 Countries* (London: London School of Economics and Political Science, 2020), available at: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf; World Health Organization Regional Office for Europe, "One in Six School-Aged Children Experiences Cyberbullying, Finds New HBSC Study," March 27, 2024, available at: https://www.who.int/europe/news-room/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study

5. Discussion and Implications

This section interprets the findings presented in the previous chapter and situates them within the broader analytical framework developed earlier in the report. Rather than treating online privacy and safety as a narrowly technical matter, the discussion below approaches these issues as social, educational, and protective concerns that require coordinated responses from parents, schools, and institutions. The workshop and training results suggest that stakeholders in Kosovo do not dismiss the seriousness of online risks; instead, the main difficulty lies in translating concern into clear, consistent, and proportionate action.

5.1 Interpreting the Findings

Taken together, the findings point to a landscape in which awareness of online risk is already relatively high, but practical readiness remains uneven. Participants generally recognized that children face real privacy and safety risks online, and they also identified a range of harms that extend beyond the digital environment itself, including embarrassment, anxiety, social withdrawal, conflict with peers, and reluctance to report problems. This confirms a central argument of the report: online harms cannot be understood only in terms of devices, apps, or settings. They are embedded in relationships, authority structures, peer dynamics, and the broader quality of adult support.

The findings also suggest that adults often stand in an ambivalent position. On the one hand, they feel a strong sense of responsibility to monitor, prevent, and react. On the other hand, they are often uncertain about where appropriate supervision ends and intrusive control begins, particularly in the case of adolescents. This tension between protection and autonomy is not unique to Kosovo; it is widely reflected in international research. In the local context, however, it appears to be intensified by a lack of practical guidance and by uncertainty around what schools and families should each do when an incident occurs.

A second important pattern is that participants did not primarily ask for more abstract awareness raising. What they consistently needed were practical tools: concrete examples, response steps, clearer school-family communication, and more confidence in how to act when a child reports a problem. This is significant. It suggests that the challenge is no longer simply persuading adults that online harms matter. The challenge is equipping them to respond in ways that are calm, proportionate, rights-respecting, and effective.

The findings therefore support a broader policy conclusion: children's online privacy and safety should not be treated as a stand-alone digital literacy issue. They sit at the intersection of child protection, education, mental well-being, and institutional preparedness. Any response that focuses only on technical controls, without addressing communication, trust, and referral pathways, is likely to remain incomplete.

5.2 Implications for Parents and Caregivers

For parents and caregivers, the findings reinforce the importance of communication as a primary protective tool. Many of the risks discussed throughout the workshop and trainings become more serious when children are afraid to speak, expect punishment, or assume that adults will react with panic rather than support. In this sense, trust is not a soft or secondary issue; it is a practical precondition for disclosure and early intervention.

This has two immediate implications. First, parents need support in moving away from either extreme permissiveness or overly punitive monitoring. Children benefit from boundaries, but boundaries are more effective when they are tied to ongoing communication, age-appropriate explanations, and predictable responses. Second, parents need clearer guidance on what to do after an incident has already occurred. In many cases, uncertainty about the right first step whether to save evidence, speak to the

child, contact the school, report a profile, or seek professional help can delay response and increase distress.

The findings also suggest that parents may underestimate the extent to which seemingly ordinary online behaviour sharing photos, participating in group chats, following peer trends, or keeping public profiles can create privacy and dignity risks over time. Practical guidance for parents therefore needs to go beyond warnings and include realistic support on digital routines, privacy settings, healthy habits, and non-judgmental conversation. The aim should not be to create constant surveillance in the home, but to strengthen informed and credible parental presence.

5.3 Implications for Teachers and Schools

The implications for teachers and schools are equally significant. Schools occupy a distinctive position: they are not only educational spaces, but also social environments in which digital conflicts often surface, intensify, or become visible. Even when an incident begins outside school grounds, its consequences may enter the classroom through humiliation, peer exclusion, concentration problems, absenteeism, or conflict between students.

For this reason, the findings support a stronger understanding of online privacy and safety as part of the school's protective and educational role. This does not mean that schools should assume sole responsibility for everything that happens online. It does mean, however, that schools need a clearer sense of what is expected of them: how to receive a report, how to document concerns, how to involve parents appropriately, when to refer to psychologists or other support mechanisms, and how to distinguish between disciplinary issues and safeguarding issues.

A further implication concerns consistency. Where individual teachers respond differently, or where staff are unsure whether a problem falls within their mandate, children and parents may experience the school as unpredictable or unhelpful. This weakens trust and reduces reporting. The findings therefore point to the need for simple, shared procedures rather than ad hoc responses. Such procedures do not need to be overly complex. On the contrary, a light but clear protocol is likely to be more usable in practice.

The findings also underline the importance of school-family coordination. Teachers cannot respond effectively if communication with parents is minimal or only occurs after a crisis. Conversely, parents may struggle to act if they do not know what support the school can realistically provide. Stronger coordination does not require formalism for its own sake; it requires clarity, timely communication, and a shared understanding that child dignity and well-being must remain central.

5.4 Implications for Institutions and Policy Actors

At the institutional level, the findings point to a need for stronger practical support around an issue that is already recognized as important. The presence of the Municipality of Prishtina, the Directorate of Education, schools, and the Agency for Information and Privacy in the broader project ecosystem reflects the fact that children's online privacy and safety cannot be addressed by individual families or schools alone. They require an enabling environment in which institutions provide guidance, legitimacy, and continuity.

One implication is that policy actors should view this field not as a niche awareness topic, but as part of broader child protection and educational governance. Institutions do not necessarily need to create entirely new structures; in many cases, the more urgent need is to translate general concern into simple operational guidance. Schools benefit from knowing what the minimum expected response looks like, where to refer concerns, and how to communicate with families in a way that is respectful, lawful, and protective.

A second implication concerns institutional continuity. One-off sessions are valuable, but they cannot by themselves sustain practice change. The findings suggest demand for continued support, whether through additional training, brief guides, model procedures, referral contacts, or repeated awareness efforts. This is particularly important in contexts where staff turnover, uneven capacity, and differing school conditions can lead to fragmented implementation.

Finally, the institutional implications extend to the policy discourse itself. Online privacy and safety should be understood as closely connected to child dignity, participation, and well-being. When addressed in this broader way, the issue becomes easier to integrate into existing child protection and education agendas, rather than being treated as a stand-alone digital concern. This framing is important if Kosovo is to move from episodic awareness raising towards a more coherent and sustainable approach.

6. Recommendations

This section translates the report's discussion into a set of practical recommendations for parents and caregivers, teachers and schools, and relevant institutional actors. The recommendations are grounded in the project findings, informed by the Kosovo context, and aligned with the international evidence reviewed in earlier sections

6.1 Recommendations for parents and caregivers

• **Strengthen regular communication and trust.** Parents and caregivers should create regular, low-pressure opportunities for discussion about children's online experiences. The findings suggest that children are more likely to disclose problems when adults respond calmly and without immediate punishment. This means that communication should not begin only after a problem occurs; it should be built into everyday routines.

• **Use clear and proportionate rules.** Household rules on device use, privacy settings, sharing of photos and personal information, and contact with strangers should be clear, age-appropriate, and explained as protective measures rather than instruments of control. Children are more likely to follow rules that are discussed and understood than rules imposed without explanation.

• **Avoid panic-based or punitive reactions.** When an online incident occurs, adults should avoid responses that focus only on blame, confiscation, or surveillance. Such reactions may stop children from reporting future incidents. A better approach is to first stabilise the situation, listen carefully, gather basic facts, and then decide on practical steps.

• **Learn simple response steps.** Parents should be familiar with a small number of practical actions: preserving evidence, adjusting privacy settings, blocking or reporting harmful users, contacting the school when relevant, and seeking professional or institutional support where necessary. The report findings indicate that adults often recognise risks but feel uncertain about how to act in practice.

• **Pay attention to behavioural changes.** Online harms do not always present as direct disclosure. Withdrawal, anxiety, disrupted sleep, irritability, reluctance to attend school, or sudden changes in device behaviour may all signal a problem. Parents should treat these changes as possible warning signs and respond with care rather than suspicion.

6.2 Recommendations for teachers and schools

• **Establish a simple response pathway.** Schools should have a basic and understandable internal pathway for dealing with online incidents that affect students, whether these occur inside or outside school but have consequences for school life. Staff should know whom to inform, how to document the issue, and when referral is needed.

• **Improve documentation and referral practice.** Teachers and school staff do not need highly complex procedures to respond effectively, but they do need consistency. Schools should use simple documentation practices, keep a record of concerning incidents, and involve the designated counsellor, psychologist, or management structure when issues exceed classroom-level handling.

• **Create a reporting-friendly school culture.** Children are more likely to seek help where they believe they will be heard, treated fairly, and protected from humiliation. Schools should therefore work to create a climate where reporting online harms is normalised and where digital incidents are treated as legitimate safeguarding and wellbeing concerns.

• **Integrate online safety into broader wellbeing efforts.** Online privacy and safety should not be treated as stand-alone technical topics. They should be discussed alongside bullying prevention,

emotional wellbeing, peer relations, respectful communication, and child protection. This approach reflects the way these problems are experienced in practice.

• **Strengthen communication with parents.** The findings suggest that school-family coordination remains uneven. Schools should therefore use parent meetings, guidance materials, and direct communication to clarify expectations, reporting pathways, and available support in relation to online harms.

6.3 Recommendations for institutions and public actors

• **Provide schools with simple guidance tools.** Relevant institutional actors, including the Municipality of Prishtina, the Education Directorate, and other competent bodies, should support schools with short, usable guidance or SOP-style materials that explain what to do when online privacy or safety incidents arise.

• **Clarify coordination and referral roles.** Institutional support should help schools understand how to connect online safety concerns with existing child protection, psychosocial support, and referral mechanisms. Clearer institutional guidance would reduce uncertainty and improve consistency across schools.

• **Support continued awareness and capacity-building.** One-off interventions are useful, but the issue requires sustained attention. Institutions should continue supporting practical awareness and capacity-building initiatives for teachers, parents, and school staff, especially where digital risks intersect with wellbeing and safeguarding concerns.

• **Treat online safety as part of broader child protection and educational wellbeing.** Public actors should avoid framing online safety as a narrow technical matter. It should be understood as part of child protection, mental wellbeing, school climate, and the right of children to participate safely in digital spaces.

• **Encourage cooperation with specialised actors.** Cooperation with bodies such as the Agency for Information and Privacy, child protection actors, psychologists, and civil society organisations can strengthen the practical ecosystem of support available to schools and families.

6.4 Recommendations for future programming and research

• **Continue adult-focused practical trainings.** Future programming should continue to focus on adults who shape children's immediate protective environment. The project findings show that parents and teachers value practical guidance that helps them respond to concrete situations rather than broad awareness messaging alone.

• **Develop school-ready tools and materials.** There is a clear need for short guidance materials, example response pathways, and practical case-based tools that schools and families can use after trainings. Follow-up outputs should therefore prioritise usability and accessibility.

• **Support further local evidence-building.** Kosovo would benefit from more systematic local research on children's online experiences, school response practices, and parent-child communication patterns. Future studies could deepen the evidence base while maintaining strong ethical safeguards.

• **Consider child participation in future phases.** Where methodologically and ethically appropriate, future phases may consider more structured and safeguarded ways of incorporating children's own voices. This would help complement adult perceptions and strengthen the local evidence base, provided that the design is carefully planned.

Recommendation matrix

Actor	Immediate priority	Medium-term priority
Parents/caregivers	Calm communication, clear rules, basic incident response	Sustained trust-building and stronger digital parenting confidence
Teachers/schools	Simple internal response pathway and reporting culture	Integration into safeguarding, wellbeing, and school-family coordination
Institutions/public actors	Short guidance and referral clarity for schools	Continued support, coordination, and evidence-building

7. Conclusion

This report has shown that children's online privacy and safety are no longer peripheral concerns. They are embedded in the ordinary realities of childhood, schooling, parenting, and peer interaction in an increasingly digital environment. The evidence reviewed in this paper, together with the findings from the workshop and training activities, points to a consistent conclusion: online harms should not be understood only as digital or technical problems, but as issues closely tied to trust, dignity, communication, well-being, and protection.

The Kosovo context reflected in this report suggests that awareness of the problem already exists. Parents, teachers, and school actors are not indifferent to online harms; rather, they often lack confidence, practical guidance, and consistent support structures. In this sense, the challenge is less one of recognition than one of response. Children need adults who are informed, composed, and able to act in ways that are both protective and respectful of privacy and trust.

For that reason, progress in this field will depend less on alarmist messaging and more on sustained, practical, and evidence-based engagement. Families need clearer tools for communication and response. Schools need simple procedures, reporting clarity, and stronger coordination with parents and referral mechanisms. Institutions need to treat online safety as part of the broader child protection and educational well-being agenda, rather than as a stand-alone technical issue.

Ultimately, the report points to a broader lesson. Protecting children online is not only about reducing exposure to harm; it is also about building an environment in which children's rights, dignity, and well-being are taken seriously across homes, schools, and institutions. A more coherent and practice-oriented response will not eliminate every risk, but it can significantly improve the conditions under which children are able to seek help, retain trust in adults, and participate more safely in digital life.


ITS
INSTITUTE FOR
TECHNOLOGY
AND SOCIETY