

## How to Ethically Promote Schools' Online Using Social Media

Carolina Piazza

[carolina.piazza@tuni.fi](mailto:carolina.piazza@tuni.fi)

Asimina Paschali

[asimina.paschali@tuni.fi](mailto:asimina.paschali@tuni.fi)

Michael Scully

[michael.scully@tuni.fi](mailto:michael.scully@tuni.fi)

Tampere University of Applied Sciences, Tampere, Finland

**Abstract:** In an increasingly digital world, schools use social media to promote their achievements and community spirit. However, using children's images and voices online requires navigating legal and ethical considerations to protect students' privacy and rights. Drawing from international frameworks such as the European General Data Protection Regulation (GDPR), the Convention on the Rights of the Child (CRC), and guidelines from international bodies, this paper explores the legal, ethical, and privacy challenges surrounding schools' social media use. It discusses the responsibilities of schools, parents, governments and the private sector in safeguarding children's rights in the digital age and calls for more awareness and comprehensive marketing practices that empower children to control their digital presence while ensuring their long-term privacy and security.

### Introduction

This paper originated from discussions exploring various aspects of post-digital education. The three authors—educators from different countries working with kindergarten and primary-aged children—consistently found that children's privacy was pervasive and deeply relevant to all aspects of post-digital education, influencing their professional practices, shaping children's perceptions, and affecting parents' expectations in all their schools. While acknowledging the increased parental involvement through social media, the authors considered the negative implications, such as safety issues, the misrepresentation of children's learning experiences, and the pressure on teachers and children to appear flawless.

Upon realizing their shared experiences, the authors began questioning the ethics of using children's personal data for schools' promotion online. Although the practice was legal—since all their schools had parents sign photo release forms—they wondered whether it was truly ethical. They questioned whether parents fully understood the implications of

sharing their children's personal data and whether it was morally acceptable to exclude children from these decisions.

In light of these considerations, the authors wrote this paper to examine recommendations from international bodies such as UNICEF (February 2018; May 2018; 2021; 2024), the United Nations (2021), and the Council of Europe (2021), with a particular focus on the European context, given the EU's leadership in data protection policies. They also reviewed existing literature to explore both legal and ethical perspectives, compiling best practices for promoting schools' online presence ethically—an area that has seen limited research in their context.

### **Privacy Concerns and Children's Rights in School Promotion**

The Human Rights Watch (2022) reported that during the COVID-19 pandemic, 49 governments recommended unsafe digital learning products for educational purposes, with 145 out of 163 products reviewed containing surveillance features to monitor children. This underscores the urgent need to protect children's privacy and rights as reliance on technology in education grows. Such concern also extends to schools' promotion on social media, which many institutions use to boost enrollments and engage parents. While the personalization and affordances of EdTech tools could benefit children, it becomes questionable whether children's best interests are truly considered when their personal data is used for marketing purposes.

Moreover, the United Nations General Comment No. 25 on children's rights in the digital environment emphasizes the need for states to uphold the Convention on the Rights of the Child (CRC) in the digital age, which highlights the interconnectedness of privacy, freedom of expression, protection from economic exploitation, and the right to development (United Nations Committee on the Rights of the Child, 2021). The CRC notes that digital tools impact children's lives and rights even when children are not the ones deciding to share their data online. This raises critical questions about the role and responsibilities of all stakeholders – parents, schools, governments, and the private sector - in managing children's data and ensuring their active participation and best interests in schools' online promotion. This paper will explore their role from both a legal and ethical standpoint.

### **Regulations and Legal Requirements**

In Europe, the General Data Protection Regulation (GDPR) plays a crucial role in protecting children's data online. UNICEF (2024) highlights the need for national frameworks to help schools understand and apply their legal duties in line with GDPR standards. Under the GDPR, schools are data controllers responsible for ensuring that children's personal data is processed in compliance with the regulation. Article 4 broadly defines data processing as any operation on personal data, including collection, storage, use, or dissemination. Schools must assess the impact of data processing on children's rights and freedoms and minimize associated risks (UNICEF, 2024).

Other key compliance steps include:

- **Consent:** Schools must obtain clear, informed consent from parents or guardians before using children's images and voices for promotional purposes. This consent should detail the usage, purpose, and display locations of the images. Children's consent should also be sought as they mature.
- **Data Minimization:** Schools should avoid sharing excessive personal information. Images should be treated as sensitive data, and their use should be carefully considered.
- **Right to Be Forgotten:** Children and parents can withdraw consent and request the deletion of personal data, including photos, at any time. This is crucial for young people, especially in an era of digital profiling, where their images and personal data may be used for commercial or surveillance purposes without their informed consent (Livingstone, 2018).
- **Record of Processing Activities:** Schools must keep a Record of Processing Activities, documenting how personal data is processed. Photos should be securely stored and accessible only to authorized personnel.

These steps align with the CRC principles, which stress treating children's data as sensitive personal data (Council of Europe, 2021). The adequacy of these procedures in protecting children's privacy rights will be discussed in the next section.

### **A Step Further – Ethical Considerations**

When promoting schools online, the ethical implications of using children's data extend beyond legal requirements.

First, children have a fundamental right to privacy, as enshrined in the Convention on the Rights of the Child (CRC). Sharing their images publicly, even with their parents' consent, can infringe on this right. Some scholars argue that parents should act as trustees for their children's digital rights, ensuring that their online presence reflects the child's best interests (Sorensen, 2020). However, parents may not fully understand the potential long-term consequences, such as creating a permanent digital footprint.

Donovan (2020) highlights how social media platforms, which have previously failed to protect user data through both unintentional data breaches and intentional circumvention of GDPR regulations, can endanger children's privacy. Moreover, the GDPR exempts household activities from privacy protections, leaving a broad gap that does not define the boundaries between parents' and children's rights. A Nominet study (2016) found that by age five, children typically have nearly 1,500 photos of themselves posted online. This exposure increases their risk of identity theft as well as economic exploitation, as these images are often used for commercial purposes without consent, thereby violating their right to protection from such exploitation (UNICEF, 2024).

This gap in the GDPR leaves children vulnerable, with no specific safeguards for their privacy and personal identity. Parents, despite being well-intentioned, may inadvertently

compromise their child's privacy, creating a digital footprint that could be exploited in the future as well as harming their children's right to self-actualization (Donovan, 2020). It is evident that merely obtaining parental consent to use children's personal data on social media is insufficient to prevent potential future harm to children. This practice should be critically re-evaluated and challenged.

Secondly, the CRC emphasizes protecting children from economic exploitation, which can be argued includes using their images in school marketing. Schools should prioritize children's best interests and dignity, ensuring photos are not used solely for their promotional gain. This is especially important when the child's consent is not involved.

Furthermore, privacy risks must be carefully examined. Every image shared online contributes to a child's digital footprint, which can have lasting consequences. As children grow, they may regret or feel uncomfortable with content shared by parents or schools. Biometric data or other personal information can be extracted from photos, creating risks like identity theft or online exploitation. Schools should limit the use of photos where biometric data may be captured and consider the potential harm to children from using their pictures online for marketing purposes.

Moreover, children, as active rights holders, should have the ability to shape their own digital identities. The practice of sharing children's images online without their involvement undermines their autonomy (Donovan, 2020) and could lead to future discomfort or even harm to their online reputation (UNICEF, February 2018).

Another consideration is whether the polished presentation of schools on social media accurately reflects the chaotic and dynamic nature of children's learning experiences or creates an illusion of perfection. This can lead to unrealistic expectations from parents and pressure on educators to present idealized events.

Lastly, UNICEF (May 2018) calls for urgent ethical standards on data privacy, product development, and marketing within the private sector. This sector, benefiting most from commodifying children's data, must prioritize these standards and be held accountable by governments and schools.

### **Best Practices to Ethically Promote Schools' Online Presence**

Considering the legal and ethical requirements, we propose the following best practices for schools to ethically promote themselves online:

- **Minimize Exposure:** Focus on school activities rather than individual children. If images are necessary, use group shots without focusing on faces or identifiable features.
- **Clear and Child-Friendly Consent:** Obtain informed consent from parents and provide children with understandable information about image use, allowing them to express preferences.

- **Authenticity:** Share photos that genuinely reflect learning experiences, avoiding misleading marketing tactics.
- **Right to Withdraw:** Make it easy for parents and children to withdraw consent and remove images from social media.
- **Data Retention:** Implement a policy to ensure images and videos are not kept longer than necessary and are deleted when no longer needed.
- **Open communication:** Be transparent about the purpose of sharing images, who will see them, and how long they will be kept online. Include image-sharing policies in parent handbooks or school agreements and maintain an open-door policy for concerns.
- **Training:** Provide guides and resources for teachers on managing children's data, understanding GDPR requirements, privacy laws, and data management.
- **Demanding accountability and transparency from social media platforms:** Familiarize with platforms' privacy policies, demand greater transparency, and choose more ethical alternatives when available.

The real-life practices in the author's schools provide insight into how these best practices were applied in varying degrees. While all schools used children's images on social media for marketing, event-sharing, and fostering community, the extent of exposure and ethical considerations varied significantly. For example, more marketing-focused schools tended to feature children's faces prominently, often emphasizing smiles over educational content. One school even used pictures of children in swimsuits, which, although not illegal, raises safety concerns and should be avoided.

In contrast, one school adhered to some of the proposed best practices by avoiding the use of children's faces, instead using images of hands or shots from behind. Their social media content had no audio, and group shots were blurred to protect children's identities, making it a strong example of ethical promotion. However, despite these efforts on social media, this school still had images of children's faces on their website, prompting internal discussions about adopting a more comprehensive ethical approach.

These case studies highlight the importance of the measures UNICEF (2024) advocates for, stressing that children's privacy needs to be safeguarded both in the short and long term as their digital identities evolve. Schools, parents, policymakers, and the private sector must work together to proactively protect children's privacy and ensure their rights are respected throughout their digital lives, especially considering the mixed practices observed in these schools.

### **Conclusion**

As the GDPR and other privacy regulations evolve, it is crucial to address the ethical, legal, and practical implications of school online promotion that involves children's digital presence. Schools, parents, and governments must work together to ensure that children's rights are upheld, particularly in relation to privacy, economic exploitation,

and self-determination. The increasing normalization of surveillance culture and the rise of the need for schools to self-promote highlight the need for stricter regulations and more robust protections for children in the digital world. Policies must adapt to ensure that children are not only protected but also empowered to make informed decisions about their digital identities as they grow.

## References

- United Nations General Assembly. (1989). Convention on the Rights of the Child. Retrieved from <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>
- Council of Europe. (2021). Guidelines on Children’s Data Protection in an Education Setting. Retrieved from [https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html#:~:text=The%20Guidelines%20on%20Children's%20Data,the%20modernised%20Convention%20108%20\(more](https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html#:~:text=The%20Guidelines%20on%20Children's%20Data,the%20modernised%20Convention%20108%20(more)
- Donovan, S. (2020). 'Sharenting': The forgotten children of the GDPR. *Peace Human Rights Governance*, 4(1), 35-59. doi:10.14658/PUPJ-PHRG-2020-1-2.
- Human Rights Watch. (2022). “How Dare They Peep into My Private Life?”: Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic. Retrieved from <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>
- Livingstone, S. (2018). Children: A special case for privacy? *Intermedia*, 46(2), 18-23. Retrieved from [https://eprints.lse.ac.uk/89706/1/Livingstone\\_Children-a-special-case-for-privacy\\_Published.pdf](https://eprints.lse.ac.uk/89706/1/Livingstone_Children-a-special-case-for-privacy_Published.pdf)
- Nominet. (2016). Parents oversharing family photos online lack basic privacy know-how. Retrieved from <https://www.nominet.uk/parents-oversharing-family-photos-online-lack-basic-privacy-know/>
- Sorensen, S. (2020). Protecting children's right to privacy in the digital age: Parents as trustees of children's rights. *Children's Legal Rights Journal*, 36(3), 156-176.
- UNICEF. (February 2018). More than 175,000 children go online for the first time every day, tapping into great opportunities. Retrieved from <https://www.unicef.org/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities>
- UNICEF. (May 2018). Children’s online privacy and freedom of expression. Retrieved from <https://www.unicef.org/childrightsandbusiness/media/291/file/UNICEF-Childrens-Online-Privacy-and-Freedom-of-Expression.pdf>

## TCC 2025 Conference Papers

- UNICEF. (2021). Policy guidance on AI for children 2.0. Retrieved from <https://www.unicef.org/innocenti/media/1341/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf>
- UNICEF. (2024). Data protection in schools: Guidance for legislators, policy makers, and schools. Retrieved from <https://www.unicef.org/eca/reports/data-protection-schools>
- United Nations Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. Retrieved from <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation#:~:text=In%20this%20general%20comment%2C%20the,the%20Optional%20Protocols%20thereto%20in>