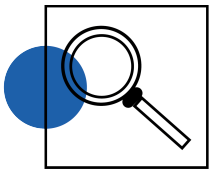
Realising children's rights in the digital age: The role of digital skills

Principle 7: Privacy

Embed privacy-by-design and data protection in policies and product development and use.



Please cite this report as: Livingstone, S., Stoilova, M., & Rahali, M. (2023). *Realising children's rights in the digital age: The role of digital skills.* KU Leuven: ySKILLS.

For full version of the report see: https://zenodo.org/doi/10.5281/zenodo.10201527

Privacy-respecting policy and innovation starts with strong data protection and privacy legislation, as well as with business models that align with lawfulness, fairness, transparency, data minimisation, purpose and storage limitations. Privacy-by-design manifests through policies and design features that give users meaningful control over the visibility, access and use of personally identifiable data. Privacy also requires legislation and security measures to prevent unauthorised access to data.[1]

The principle of privacy-by-design draws on children's right to the protection of privacy and image, requiring responsible handling of personal data, including:

- Deployment of appropriate security measures to guard against unauthorised access to personal data.
- Compliance with data protection principles of lawfulness, fairness, transparency, data minimisation, accuracy, purpose and storage limitation.
- Respect for children's agency, dignity and safety in the sharing and use of children's data.

Threats to children's right to privacy and data protection in the digital environment manifest in three domains: interpersonal, institutional (e.g., education, health) and commercial (Stoilova et al., 2021). In each domain, specific considerations apply to ensure children's privacy is protected along with their other rights.

"It's almost absurd, I was searching for a computer and I visited an online shop and suddenly I had computer ads everywhere, so they're definitely tracking me." (teenager, Czech Republic) (24)

[1] UNCRC, Article 16.

"On Instagram, I have two accounts. I have a more public account that has more people that I might not be close with. But I also have a private account with, like, 20 people, like, my closest friends. I feel like I can reveal a bit more about myself on my private account." (teenager experiencing mental health difficulties, UK) (17)

In the digital age, the right to privacy is in practice increasingly being managed through data protection regulation, whether or not appropriately. This puts a focus on data-related aspects of privacy, leaving other areas such as physical or psychological integrity, identity building or sexuality to other regulations, not necessarily deriving from the digital environment. Important in this regard is framing the child as a data subject, for which digital skills are needed if children are to access their data subject rights vis-à-vis those organisations that collect, store and share their personal data. Privacy is not simply a matter of having control over one's data, however, and judgement of what is public or private is heavily contextual. At least three contexts are important for children – interpersonal (including family, peers, online publics and strangers), institutional (such as data held by the child's school, doctor or other health provider, or public transport system) and commercial (encompassing a host of businesses – those that are primarily digital such as social media companies or search engines and also those that operate in digital contexts – banks, shops, entertainment providers, advertisers, insurers, data brokers, and more). This results in a highly complex and often opaque set of contexts within which children's rights to privacy may be respected or infringed. It also implies the need for a demanding set of digital skills and literacies if children are to play an active role in exercising and defending their right to privacy (Stoilova et al., 2021).

The findings from ySKILLS research show that **children with higher levels of digital skills may be better able to protect their privacy online** (14). The qualitative research shows how children value the skills to manage their privacy online – for instance, a number of refugee children and young people reported that they have ensured their settings are private, blocked individuals and/or adjusted their practices to avoid harmful content (26). Relatedly, children and young people experiencing mental health difficulties reported both heightened attention to online privacy, but also a host of challenges when their privacy was infringed (17).

Overall findings from the survey show that **a majority of children (83%; N=6,022) report that they know how to adjust their privacy settings online**, and nearly as many have used them (for instance, 78% limit how many people can see their social media profile) (d'Haenens et al., 2023). The ySKILLS performance tests broadly confirmed these encouraging findings, showing, for example, that, when asked which of four posts was not okay to share with others without asking for permission first, 73% of children selected the right post. However, the report observes that one-third of the participating children and young people 'do not consider blocking an unknown person who's sending nasty comments' and most 'do not have the skills to choose the right settings in an online meeting or to send a message appropriate to the situation' (22:32).

Notably, the ySKILLS research prioritised skills to manage interpersonal privacy. Further research is needed to understand children's capacity to manage how their data are processed by institutions and businesses, insofar as such management is made possible for users by the digital design of these organisations, although the qualitative studies did reveal that children and young people are often aware that platforms track their behaviour, and that the content they get presented with is based on this tracking (17, 24, 26). Further analysis of ySKILLS findings is also needed to understand the role that digital skills (including, but not limited to, skills specifically relating to privacy) may play in improving children's privacy online.

Additional data

EU Kids Online findings for 9- to 16-year-olds in 19 countries showed that:

- One in five children said their parents had published something online about them without asking them first.

- Across countries, an average of 7% of children said someone had used their password to access their information or pretended to be them, 7% said somebody had used their personal information in a way they didn't like, and 5% said someone had found out had where they were because they had tracked their phone or device.

- Fifteen per cent of children said their parents used technology to track their location – more younger than older children, with no clear gender differences.

- Four in five children aged 12–16 said they knew how to change their privacy settings, and even more said they knew which information they should and shouldn't share online and how to remove people from their contact lists.