

A group of four children are running away from the camera through a grassy field towards a line of trees. The child in the center is a boy wearing a blue and white striped t-shirt and khaki shorts, carrying a large blue backpack. To his left are two girls, one in a light blue patterned top and the other in a light blue top and denim shorts. To his right is a girl in a blue t-shirt and khaki shorts, also carrying a blue backpack. The scene is bright and sunny, with dappled light on the grass.

HARMFUL SHARENTING IN THE UK

Protecting children from digital harm

Context

Sharenting - the sharing of children’s personal information by parents on social media - has become a widespread practice. While often well-intentioned, it exposes children to harm. Examples include identity-related crimes, harassment, cyberbullying, contact by strangers, and privacy breaches. The **ProTechThem** interdisciplinary research project brings together social and computer science expertise to investigate sharenting risks. The project reveals that current regulations, platforms’ safety provisions, and parental cybersecurity measures are insufficient to protect affected children from digital harm. This brief outlines key harms of sharenting and proposes both evidence-based and actionable policy recommendations for a safer digital future.



Key Findings

45%

Prevalence:

45% of UK parents practice sharenting



Commonly used platforms:

Facebook, Instagram, TikTok



Data shared:

Photos, birthdays, health updates, school milestones



Victimisation:

1 in 6 reported negative incidents affecting children (identity-related crimes, cyberbullying, contact from strangers, and privacy breaches)



Motivations:

Emotional connection, social capital, informal advice-seeking, monetisation



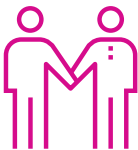
Risky behaviours:

Public sharing, weak privacy settings, frequent posting



Platform vulnerabilities:

Easy re-shareability of children’s information across social media, inaccessible privacy policies.



False sense of security:

Parents overestimate the effectiveness of platforms’ privacy tools

Key Challenges



- **Children’s Rights and Digital Exposure:** Children’s right to privacy (UNCRC Articles 8 and 12) is often unintentionally violated through online disclosures. Personal and sensitive data accessible through the information parents share about their children (such as location and birth date) can be misused by malicious actors to harm children.
- **Parental Awareness and Misplaced Trust in Platforms:** Our survey of a nationally representative sample of 1013 UK parents and interviews with 30 found a major gap in cybersecurity awareness, with many parents overestimating platform safeguards such as private settings.
- **Weak Platform Accountability and Regulatory Gaps:** Social media platforms lack robust privacy-by-design mechanisms. Current legal frameworks (The Online Safety Act 2023 and The UK General Data Protection Regulation - GDPR) do not explicitly address the specific harms of sharenting, leaving regulators, educators, and parents without clear guidance.

Typology of Sharenting Harms Affecting Children



Identity Fraud



Identity Theft



Harassment



Cyberbullying



Contact by Strangers



Privacy Breaches

Recommendations

Policy Makers, regulators, and legislators:

1. Establish a Coordinated UK Risk Mitigation

Strategy: Convene a multi-stakeholder taskforce including Ofcom, DCMS, ICO, Children's Commissioner, NGOs, and schools; Embed children's rights into digital parenting guidance, modelled on UNCRC Articles 8 & 12.

2. Strengthen Platform Responsibilities:

Mandate the sharing of child-specific content to be private-by-default; Mandate platform data protection audits focusing on sensitive child-specific content (images and other information); Mandate platforms to publish annual data on sharenting-related incidents; Require platforms to publish plain-language safety notices or pop-ups during child content uploads.

3. Build Parental Cybersecurity Awareness:

Integrate ProTechThem's Sharenting Risk Awareness Checklist into national online safety curriculums and parenting classes; Support co-branded campaigns between schools, NGOs, and tech companies.

4. Regulate Criminogenic Affordances:

Expand the Online Safety Act to explicitly include sharenting-related harms; Ban platform practices that algorithmically amplify child-centric content to inappropriate audiences.

5. Create an Independent Ombudsman for Child Data Harms:

Establish a Children's Data and Privacy Ombudsman, empowered to receive complaints, advise families, and issue guidance to platforms and other digital service providers. The existing Local Government and Social Care Ombudsman focuses on child protection issues and Ofcom, the UK's independent media regulator, does not provide the proposed service.

6. Introduce centralised control:

Bring sharenting under the oversight of the Children's Commissioners for England and Wales.

7. Invest in Interdisciplinary Sociotechnical Tools:

Fund development and deployment of AI tools for sharenting risk detection; Encourage platform adoption of Natural Language Processing (NLP) moderation systems: These can flag sensitive child-related posts. The ProTechThem interdisciplinary research project is developing a digital system based on Large Language Models (LLMs).

Police:

8. Train police & social workers on digital harms and privacy rights under the UK GDPR and UNCRC.

Educators:

9. Incorporate sharenting risk awareness into school ICT curricula: Collaborate with Ofsted
10. Train teachers and parents on digital harms and privacy rights
11. Review Schools' use of social media in line with our findings and recommendations

Service Providers:

12. Embed proactive pop-ups/reminders that are triggered by child-centric uploads.
13. Perform audits on data protection mechanisms for children affected by sharenting.
14. Publish annual data on sharenting-related incidents.
15. Partner with law enforcement and NGOs to test and refine automated risk detection systems; Develop a cross-sectoral taskforce to monitor tech developments and associated risks.

Lead Researchers

Prof Pamela Ugwu-dike | University of Southampton

Prof Silke Roth | University of Southampton

Dr Anita Lavorgna | University of Bologna

Dr Stuart E. Middleton | University of Southampton

Research Fellow

Dr Natalie Djohari | University of Southampton

Research Collaborator

Dr Morena Tartari | Northumbria University



Find out more

This policy brief draws on interdisciplinary research funded by ESRC [ES/V011278/1] conducted by the University of Southampton in partnership with the UK's DCMS, NGOs, and child safety organisations. **ProTechThem: Building Awareness for Safer and Technology-Savvy Sharenting**

DOI

doi.org/10.5258/SOTON/PP0118

Harmful sharenting in the UK: Protecting children from digital harm - **<https://10.5258/SOTON/PP0118>**

Contact

Email: **p.ugwu-dike@soton.ac.uk**

Website: **www.protechthem.ac.uk**

