Press release and backgrounder

SOCIAL MEDIA IN EDUCATIONAL SETTINGS: A CALL FOR GOVERNMENTS TO ISSUE GUIDANCE TO PROTECT CHILDREN AND RAISE AWARENESS OF THE RISKS

UK school children's photos are being scraped from websites and included in AI training datasets. Schools are increasingly using social media to publish pupils' photos to celebrate their achievements. Original analysis of Freedom of Information requests sent to every Local Education Authority in England, Wales and Scotland, reveals that the consent forms and privacy notices recommended to schools very rarely mention risks posed to children from schools' use of social media. We make recommendations on how educational settings can ensure families understand how and where children's personal information is being shared and can weigh up the risks and benefits to protect children, in line with emerging threats.

RESEARCH FINDINGS FROM DR. CLAIRE BESSANT

Dr. Claire Bessant, Associate Professor at Northumbria University, Law Department asked Local Authorities in England, Scotland, and Wales with responsibility for education, what guidance they provide to schools on their use of children's images on school social media.

Of the 205 Local Education Authorities asked, 190 replied but the vast majority (125) advised that they were unable or unwilling to provide a substantive response. 65 authorities supplied copies of their guidance, privacy notices and consent forms. The documents disclosed suggest confusion about the information schools should provide to parents and whether or when schools should seek children's views and at what age.

- Thirty-five authorities (54%) suggested consent is obtained only from parents. Where authorities suggested consent should be obtained from children, the recommended age to ask the child varied wildly from age 8 to 16.
- Information sheets and consent forms rarely state why children's images are being used and how exactly children's images will be used or on what platforms. Schools should clearly explain to children/parents what they are consenting to and explain all of the risks once photographs are outside a school's control, in a way they can easily understand. Where schools fail to do so, they do not meet UK General Data Protection Regulation requirements and consent is invalid.
- 19 authorities suggested schools should seek a blanket consent for all online image use.
- Only 5 authorities suggested parents should be able to choose on which social media platforms their children's images appear and decline others.
- **Of the 65 authorities who replied and provided documentation, only 7% discussed risks and consequences of the photos being posted on schools' social media accounts.**
- **Less than 1/3 of those authorities (10% of all authorities) outlined safeguards to protect children's privacy and safety.** Safeguards mentioned included not providing a child's name alongside their image or ensuring children are suitably clothed. This, however, wrongly assures parents of safe practice by suggesting that leaving out personal information about the child, such as name, means they cannot be identified.
- Any advice offered was limited to explanations that once shared, images are outside the schools' control, accessible to the general public, and therefore may be misused. They all failed to fully explain how images might be mis-used by third parties and how this might impact on a child.

Some Authorities gave good advice to educational settings, such as the East Dunbartonshire LEA noting, **"images used on internet/websites have the capability of being viewed by any person with internet access worldwide. The school cannot control who will view the images or the countries in which the images may be accessible**."

Advice could still, however, be more specific. In April this year, 2024, the Welsh government website published guidance for schools reminding them that, **"any image publicly published can be copied, downloaded, screenshotted or shared by anyone. These images may be adapted and used inappropriately,"** and that, **"The potential risks of digital exposure can last a lifetime."**[1]

Some authorities also provided concerning advice. Durham City Council suggested **children may be excluded from taking "full part in some school events" unless permission is granted for the taking and use of images**. Since consent must be freely given in order to be valid, it means that parents/children have a genuine choice. Where parents/children cannot refuse consent without detriment, consent will not be valid and this suggestion by Durham therefore invalidates its consent process.

THE RISKS

Where a pupil goes to school can be inferred from a school's social media posts. Many children are identifiable to strangers even without their names or school name being included alongside images.

Digital rights campaign group Defend Digital Me has found in September 2024 that the risks are not only theoretical. LAION-5B, a dataset used to train popular AI tools and built by scraping most of the internet, contains links to identifiable photos of UK school children of all ages. Sometimes children's names and their school are listed in the image caption or in the URL where the image is stored.[2]

Separate research about where AI training datasets are sourced from around the world, carried out and published by Human Rights Watch in summer 2024, similarly found links to identifiable photos of school children from Australia and Brazil. In many cases, their identities are easily traceable, including information on when and where the child was at the time their photo was taken. In one case found, a child's contact telephone number is made public, contained in the training dataset.

By posting children's facial photos online, schools can unintentionally compromise children's privacy and expose them to risks of identity fraud, harassment and grooming, image theft and abuse. Information and images shared on social media platforms may be harvested, manipulated, linked with more personal data and used to make assumptions, profiles or predictions. Children cannot control how their images are used or easily remove them, if at all, after the photos have been made public.

The sharing of children's images on educational settings' social media sites, also contributes to a child's lifetime digital shadow[3], the data associated with children that we cannot see, that can be used to make assumptions and predictions about individuals and groups of children.

RECOMMENDATIONS

Drawing on advice from the UK Information Commissioner, from the UN Committee on the Rights of the Child and the Welsh Government website Hwb, and recognising that education is devolved:

For Departments for Education and policy makers

The UK governments should consider the issues and publish statutory guidance in consultation with representatives from the devolved nations, education unions, educational settings, the Information Commissioner's Office, academics and other stakeholders with interests in human rights to ensure the rights of the child are prioritised above schools' marketing and promotional materials, or social media presence.

Strong protection is currently afforded to biometric data, eg using children's photographs in cashless catering systems, but is not currently provided to children's photographs online - given the risks posed to children by the online dissemination of their images children's photographs should be given the same respect as biometric data. Valid consent for processing photographs can only be obtained where children/parents fully understand the risks posed by the online publication of children's photographs – the Department of Education has a key role to play in ensuring education professionals and educational settings understand these risks and are able to explain them to children and parents.

Teachers should be provided with continuous professional development on data and digital rights and their own responsibilities, and these topics should be added to the curriculum in initial teacher training.

[1] Hwb (2024) What schools need to know about web scraping
https://hwb.gov.wales/keeping-safe-online/what-schools-need-to-know-about-web-scraping

[2] Source: https://spawning.ai/have-i-been-trained

[3] Understanding your digital shadow https://www.uow.edu.au/student/support-services/academic-skills/online-resources/technology-and-software/understanding-your-digital-shadow/

For Educational Settings and Authorities

To limit exposure of distribution beyond the school community, staff may make sections of the school website and all social media settings private. Understand however that this has limited benefit because images may still be scraped remotely or copied and posted elsewhere by people among approved users.

Schools could instead reduce exposure at source by using photographs showing students at a distance, in groups with indistinct faces, or with faces angled away from the camera. Risks of identification may be reduced if children's names are not used, but their face is a key identifier.

Under current data protection law, to ensure children can express their views as their capacities develop, regular (annual) renewal of consent should be considered. Schools should also use informal opportunities to explore their children's and community views on whether their photographs are taken or shared by others at school and by parents.

Children and parents must be fully informed about how educational settings wish to use children's images, and children should have an opportunity to express their views. Even where parental consent is sought, schools must also provide children with age-appropriate information about how schools use their images in line with current data protection law. Parental consent forms should encourage parents to discuss with their children how schools use children's images at all images. Schools themselves should also, as part of their digital literacy role, be discussing with children how their images will be used, not just by third parties, but by schools themselves.

When it comes to distribution, parents and children should be able to choose whether images are shared only in printed publications, on school premises, or digitally with other parents with accepted terms of use, or published on school websites or on specific public social media platforms where privacy risks may be greater. Blanket consent forms to all-or-nothing are not valid and should not be used.

If the law or guidance were changed to improve current practice and were based on current law on biometrics in schools, authorities would ensure that a child's information is not processed unless at least one parent of the child consents to the information being processed, and no parent of the child has withdrawn their consent, or otherwise objected. And if, at any time, the child refuses to participate in, or continue to participate in, anything that involves the processing of the child's information, or otherwise objects, the relevant authority must ensure that the information is not processed, irrespective of any prior consent given by either parent of the child.

For Families

Before granting permission for children's photos to be used by an educational setting, parents should consider children's digital footprint for life, not only for them as a child at that point in time.

Parents should be made aware that where schools share children's images on social media platforms this may inadvertently expose children to risk of harassment, grooming, image theft and abuse, and identity fraud for life. Information and images shared on social media platforms may be manipulated, harvested, linked with more personal data and used to make assumptions or predictions.

Once a photograph is published online, it is available to high-speed automated scraping tools and could be used by strangers including images they obtain to create AI training datasets, and retained forever by strangers and which may be used for purposes you will not ever see, including to create databases for training and creating non-consensual images.

Parents need to consider children's further education, future employment, and reputational risks and how they may be negatively impacted as a result.

QUOTES

Quote from Dr Claire Bessant

It is concerning that many education authorities' provide guidance to schools which fails to explicitly recognise that significant risks may be posed to children by the online dissemination of their photographs. Some of this guidance appears to illustrate only a partial understanding of UK data protection laws, where schools seek consent to use a child's photograph. There is an urgent need for national level guidance to be provided by the Department of Education and/or the Information Commissioner.

Quote from Jen Persson, Director Defend Digital Me.

Posting children's photos online including on school social media sites is a risky business. Dr Bessant's research shows that people working in the public sector with children's best interests at heart, are very often untrained, and unaware of the risks their everyday practices create. It's all very well banning the production of images but scraping won't stop. The photos need to not be there in the first place. To stop putting children at unnecessary risk, educational settings must change their own habits, the Department for Education needs to issue urgent guidance, and the government must put a Code of Practice into law for educational settings.

APPENDIX: PHOTOS OF UK SCHOOL CHILDREN FOUND IN AI TRAINING DATASETS

Can be discussed and viewed on request.

CONTACT DETAILS

Dr. Claire Bessant
Associate Professor, Northumbria University, School of Law
claire.bessant@northumbria.ac.uk
https://researchportal.northumbria.ac.uk/en/persons/claire-bessant

Northumbria University NEWCASTLE

For the full academic research paper see: 'School social media use and its impact upon children's rights to privacy and autonomy' (2024) *Computers and Education Open: Datafied by Default: Examining the Intersect Between Children's Digital Rights and Education* https://doi.org/10.1016/j.caeo.2024.100185

Original Freedom of Information requests and responses can be found in the disclosure logs published by individual education authorities on their websites.

Jen Persson
Director, Defend Digital Me
07510 889833
jen@defenddigitalme.org
https://defenddigitalme.org/

defend|digital|me

Defend Digital Me is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond.

LAUNCH EVENT DETAILS

Monday November 18th, 5.30-7pm. Houses of Parliament Committee Room 4. On the eve of the Second Reading of UK data protection reform, and in the week of World Children's Day.

https://www.eventbrite.co.uk/e/childrens-data-use-and-access-in-educational-settings-in-the-context-of-ai-tickets-1076171711559