Hampshire County Council

Improvement and Advisory Service

Non-statutory guidance on the use of pupil identifiable imagery in public-facing media

Balancing cybersecurity, safeguarding and communication risk

For many years, schools in Hampshire have published pupil photographs and videos publicly for a wide range of positive reasons, including celebrating learning, sharing school life and strengthening parental engagement. Schools have generally done this carefully, balancing risk through parental consent and by avoiding obvious identifying information, such as pupils' names or classes. In the past, these mitigations often made carefully curated public photographs and videos feel proportionate.

That risk balance has now changed. Ordinary photographs and videos of pupils can be misused in ways that were not previously easy to access. Images showing pupils' faces can be copied from school websites, manipulated using AI tools to create sexualised abuse images, and then used to blackmail the school, humiliate the child or cause wider safeguarding harm.

Publicly accessible pupil identifiable imagery now carries increased risks, including safeguarding harm, distress, humiliation, reputational damage, blackmail, grooming, peer misuse and data protection concerns.

Due to the increased risks of AI-created child sexual abuse material, blackmail threats and the other risks identified in Table 1 below, Hampshire Improvement and Advisory Service (HIAS) advises that school leaders review the use of pupil identifiable imagery on public facing school communications of any type including school websites and school social media. This may involve moving towards using anonymous pupil media, or images of the school environment where pupils are not present. Recommended actions are set out in Table 2 below.

This advice is based on balancing the benefits of public communication against the possible harms. Schools are free to make their own decisions. However, we strongly advise any school that continues publishing pupil-identifiable imagery to update its consent processes so that parents and carers are clearly informed of the potential risks.

Sharing identifiable imagery with parents through a secure school portal or learning platform may allow schools to continue sharing learning with reduced risk, provided all stakeholders understand that identifiable images must not be downloaded, copied or shared outside the platform.

Key terms

Identifiable imagery means pictures or videos that include pupils' faces, or that allow a pupil to be identified through context.

Anonymous pupil media means pictures or videos that show pupils' learning or activity without showing pupils' faces or other identifying details.

Embedded metadata means hidden data attached to a photo or video file. This may include the date, time, location and device used.

CSAM means child sexual abuse material.

Table 1: Risks posed by identifiable imagery or embedded metadata on school websites, social media or communications

Risk	How it could happen	Why it matters for schools
AI nudification or deepfake abuse	A face or image is copied from a school website and used in an AI tool to create fake sexualised CSAM imagery.	The resulting harm can be serious, causing distress to the child, anxiety for families, safeguarding concerns and reputational damage for the school.
Financial blackmail of the school	Criminals send AI manipulated CSAM images to the school and threaten publication unless money is paid.	Schools could be placed in an extremely difficult position, balancing pupil safety against the risk of rewarding blackmail.
Blackmail of an individual pupil	Sextortion is a growing form of online blackmail involving real, hacked or AI generated images.	Schools may be seen as responsible if a pupil image published by the school is later misused to blackmail a family, creating safeguarding, wellbeing and reputational risks.
Grooming or targeting	A pupil is identifiable through face, name, uniform, club, year group, award, team, school or location.	Online images can help identify children for future grooming, targeting or abuse. Schools would not want to be identified with this.
Risk to looked after children or vulnerable pupils	Public images reveal that a child attends a specific school or event.	Schools have a duty of care to avoid revealing the location of looked after children, adopted children or those protected by a court order.

Metadata exposure	EXIF data reveals location, device details or timestamps.	Embedded metadata can provide additional information about the location of school or off-site events which can increase safeguarding risks to pupils.
Searchability and permanence	Images appear in search results, are archived, downloaded, screenshotted or reposted.	Once an image is publicly available, recalling it is extremely difficult. Schools will avoid this issue by using anonymous pupil media.
Unintended identification through context	A seemingly safe photo is combined with captions, names, house teams, sports fixtures, uniform, certificates or location tags.	The safeguarding risk is not only the image itself, but the wider data trail around it which might provide additional information that criminals might use to target the school or pupil.
Peer misuse	Pupils download official school images and alter, meme, mock or sexualise them.	AI generated or digitally manipulated pupil images are now part of the wider nude and semi-nude incident landscape. Schools publishing identifiable imagery may be contributing to this.
Reputational and emotional harm	A manipulated image circulates among peers or online communities.	Pupils may experience fear, distress, shame, reputational harm, peer exclusion through repeated victimisation, creating a serious safeguarding and wellbeing concern.
Staff and over 18 pupil risk	Staff photos or key stage 5 images are misused in similar ways.	Adult staff and pupils over 18 may feel that the school did not do enough to protect their image and reputation which might prompt litigation.
Data protection breach	Images are used beyond the purpose explained to families, retained too long or shared too widely.	Identifiable images are personal data and must be handled in line with data protection principles to avoid censure and a fine.

Table 2: Recommended actions

Treat pupil-identifiable imagery as a **safeguarding, data protection, and communications risk**, in addition to a consent issue.

Suggested actions:

1. Audit all publicly identifiable pupil images on the school website, social media, prospectus pages, news posts, PDFs, and archived newsletters.
2. Consider replacing pupil-identifiable images with anonymous pupil media, such as backs of heads, over-the-shoulder work, hands using equipment, displays, classroom resources, or any image that cannot be misused.
3. Review photo consent forms so parents and pupils are clearly told about AI manipulation, image retention risks, onward sharing risks, social media risks and the right to withdraw consent.
4. Consider limiting pupil-identifiable imagery to use only within the school's physical confines, for displays, etc or within a school portal or learning platform.
5. Add pupil-identifiable image security to the safeguarding policy, online safety policy, acceptable use policy, social media policy, and staff induction.
6. Continue to train staff not to use personal phones or personal cloud accounts for school images.
7. Have a response plan for peer misuse, manipulated or blackmail-related imagery, including DSL escalation, police contact, secure evidence handling, parent communication, pupil support, and the use of Report Remove or other removal routes.

Further Reading
https://saferinternet.org.uk/blog/schools-given-advice-on-image-safety-to-keep-ahead-of-threat-from-ai-blackmailers

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion

https://www.theguardian.com/technology/2026/may/08/uk-schools-remove-pupils-photos-online-ai-blackmail-threat-grows

https://www.gov.uk/guidance/data-protection-in-schools/taking-and-using-photos-and-videos-and-using-cctv-in-schools

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

https://learning.nspcc.org.uk/online-safety/photographing-filming-children

Phil Bagge Computing & AI Inspector/Advisor 14/05/2026
V4