Protecting your setting's images from AI manipulation and abuse:

Guidance for education settings and organisations working with children and young people

Developed by the UK Online Harms Early Warning Working Group, this guidance shares best practice and considerations for education settings and organisations working with children and young people on the use of photos and videos of children and young people across their online platforms, to address the risk of AI image manipulation.

Practices to protect young people's images

This document looks at the responsible management, sharing and protection of photographs and videos, particularly those featuring children and young people. This includes images used across education settings' websites, social media platforms and other digital spaces. When thinking about how to best protect children and young people's images online, schools and education settings may wish to think about image security practices such as:

- **Ensuring images do not contain identifiable information** that could be used to harm or blackmail an individual (e.g. full names or faces).
- **Using imagery that is harder to misuse or abuse**, this could be by only sharing photos taken from a distance, blurred images or images taken from over the shoulder.
- **Applying privacy settings** to help limit who can view and share content (this can be done on social media or any other place the images are stored or shared).
- **Removing metadata** (e.g. EXIF data) from the images that may reveal location, device details or timestamps. Such data can unintentionally reveal schedules or routines, for example of regular training
- **Embedding image security awareness and practices** in staff training and policies.

What are the risks?

Ensuring images of children and young people are protected is not only about compliance or reputation but, most importantly, safeguarding. The duty to safeguard children and young people includes online spaces.

Risks associated with poor image security may include:

- **Misuse or abuse of images:** images of children and young people may be taken from education settings' websites or online platforms, for example via web-scraping. These images may be misused, shared without consent or manipulated to create further imagery of children and young people, including the use of AI tools such as nudification apps to create child sexual abuse material (AI CSAM).

- **Vulnerability to blackmail:** misuse or abuse of images, particularly AI CSAM, may be used to blackmail education settings or individuals to pay money against the threat of sharing of these images. Images of children and young people (or staff) may be vulnerable to this type of blackmail.

- **Safeguarding concerns:** the potential misuse, abuse or sharing of images of children and young people without consent can lead to safeguarding concerns, for example, Looked After Children. This may include vulnerability to online blackmail or putting children and young people at risk of harm by exposing personal information or location data.

- **Privacy breaches:** loss of control of metadata that exposes sensitive information can lead to data and privacy breaches.

Why is this important?

Putting in place image security measures and carefully considering how and what imagery of children and young people is used is important for a number of reasons, including:

- **Safeguarding children and young people:** safeguarding should be the highest priority for education settings when using children and young people's imagery. Advancements in online technology create new vulnerabilities and capabilities that can lead to children and young people's images being misused, shared without consent or exposing personal data. It's important that education settings understand these risks and put a safeguarding-first approach in place to protect children and young people.

- **Building trust:** putting measures in place to protect student image security demonstrates a commitment to privacy, safeguarding and responsible digital practices. It can build greater trust with children, young people, parents, carers, governors and inspectors.

- **Celebrating achievements more safely:** image security is important to ensure education settings are able to showcase their environment, student life and achievements while minimising risks.

- **Compliance:** image security supports alignment and compliance with data protection legislation and local authority policies.

Checklist of actions to consider

Staff training and response:

- [ ] All staff should be trained to recognise and respond to incidents of image-based abuse (e.g. non-consensual sharing, manipulation or threats involving student imagery) with emphasis on prevention and safe practice.
- [ ] Ensure any immediate safeguarding response prioritises the student's safety, dignity and emotional wellbeing.
- [ ] Report any blackmail or threats involving imagery to the police as a criminal matter, alongside following internal safeguarding procedures.

Parental consent:

- [ ] Provide parents, carers and young people with clear information about the potential risks of image use, including the online misuse and manipulation of digital content, and the steps your setting is taking to mitigate this.
- [ ] Review and re-sign consent forms for photographs and videos regularly (e.g. annually or at key transition points) to ensure ongoing awareness and agreement.
- [ ] As best practice, children and young people should give their own consent in addition to parental/carer consent, recognising their growing autonomy and rights, if they are old enough and have the capacity to make their own decisions.
- [ ] Ensure consent forms are fully accessible, with opportunities for questions and withdrawal at any time.

Content renewal and audits:

- [ ] Schedule regular, documented audits of children and young people's imagery (e.g. termly or biannual) on websites, social media and promotional materials.
- [ ] Ensure any out of date images are updated or removed where necessary to minimise risk, and that this process aligns with current consent and safeguarding guidance.
- [ ] Update policy and practice guidance to ensure good digital practices in relation to data minimisation and storage limitation obligations. You should only retain personal data for as long as necessary and limit the amount of data collected, including student imagery

Key question to consider: Are images of children and young people needed?

To protect your setting, staff, and young people, consider whether children and young people's images are required at all, or whether using imagery without children and young people's faces can still achieve your objectives (e.g. showcasing your setting).

If you are using images of children and young people, you should also consider the following:

- [ ] Replacing images that directly show a student face-on, using alternative angles that minimise identifiable features.
- [ ] Avoid names or full names.
- [ ] Limit public visibility of student images (e.g. closed groups rather than open platforms).
- [ ] Ensure all image metadata is stripped before publication.
- [ ] Use lower resolution images to reduce risk of misuse.
- [ ] Share clear information with parents and carers about potential risks and the processes in place to protect student imagery.
- [ ] Embed image security into policy and procedure, making it a standing requirement across safeguarding, communications and IT practices.
- [ ] Consider protective software solutions (e.g. watermarking, metadata scrubbing or "immunisation" tools) to reduce the risk of unauthorised alteration or misuse of student imagery.
- [ ] Replace images of any children or young people who are no longer members of the school community.

What to do if images of young people are misused, altered or abused

If an incident occurs, it is important to take the following steps:

Contain & Escalate

- [ ] Do not delete or further share any communication or criminal images relating to the incident. Retain and store securely and seek advice from your local police force.
- [ ] Immediately ensure the original version of the compromised images are no longer publicly available, including on websites or social media.
- [ ] Notify your school or organisation's Designated Safeguarding Lead/Person or a senior colleague.
- [ ] Record details of the breach in line with your standard incident reporting processes, including carrying out a risk assessment of the impact on individuals and taking any notification actions as required.
- [ ] If you have been approached with demands by someone attempting to blackmail your setting, it is important that you do not engage with the individual or respond to any of the demands. The paying of ransom can be illegal in certain circumstances.

Report

- [ ] **Police:** Report to your local police force if you have received threats to publish sexual imagery of children or young people in your educational setting. The creation of child sexual abuse material is illegal regardless of whether it is AI-generated or not. If a young person is at immediate risk of significant harm, call 999.
- [ ] **Report Remove (Childline/IWF)**: Support under-18s to use the confidential 'Report Remove' tool to report sexual images or videos of themselves, including if they are created by AI, to see if they can be removed from the internet.
- [ ] **Take It Down:** An image take down service, including for AI-generated images, offered by the National Center for Missing and Exploited Children (NCMEC).
- [ ] **Stop NCII:** Use 'Stop NCII' for the removal of non-consensual intimate images of over-18s, whether pupils or staff, including if these images are generated by AI.

Platform reporting

- [ ] Request removal from hosting sites/social media where the images have been shared.

Support

- [ ] Prioritise student safety and wellbeing.
- [ ] Inform parents and carers with clear next steps.
- [ ] Exposure to illegal material involving children, and responding to concerns while supporting affected families, can be extremely distressing for the staff involved. It is therefore important that affected staff are made aware of the wellbeing support available to them through their employment or external helplines. Professionals, parents and carers can also seek support and advice via the Stop It Now helpline or the Professionals Online Safety Helpline.

Prevent Recurrence

- [ ] Audit imagery on school websites/platforms and tighten consent processes.
- [ ] Update policies and staff training.
- [ ] Consider protective software (e.g. watermarking, metadata scrubbing).

What to do if someone over 18 is targeted

Some young people will be over 18 whilst still at school or college and it is important that they are made aware of the support tools that they can use. Staff can be targeted and are also able to make use of these reporting routes and support services.

Anyone 18 or over who is being threatened with the release of their intimate images can contact Stop NCII and the Revenge Porn Helpline.

Guidance for higher education professionals can be found here: FMSE HE 18+ guidance and poster

Helpful guides and tools

- Guide to removing EXIF metadata - A guide created by the early warning working group.
- Hwb: Practices and principles for schools' use of social media - A guide to support schools and education settings in the safe and responsible use of social media.
- ICO: Data sharing code of practice - Practical steps that individuals, businesses and organisations need to take to share data while protecting people's privacy
- ICO: A guide to data security - Guidance on how organisations should approach data security under UK GDPR, outlining practical steps to protect personal data.
- Internet Watch Foundation - Anonymously report suspected child sexual abuse images or videos.
- IWF and NCA CEOP Education guidance: Understanding and responding to AI-generated child sexual abuse material - Information for all professionals working with children and young people.
- Marie Collins Foundation: Supporting children impacted by image abuse - a free resource that addresses some of the recovery needs of a child harmed by Technology-Assisted Child Sexual Abuse.
- Professionals Online Safety Helpline - Supporting professionals working with children and young people, with any online safety issue they may be having.
- Report Remove - Helping young people under 18 in the UK to confidentially report sexual images and videos of themselves and remove them from the internet.
- Risk assessment template - An example risk management template which setting can adapt to meet local need.
- SBNI Online Safety Hub AI misuse guidance: Northern Ireland - Explaining how AI can be misused, and highlights the key safeguarding concerns that parents, carers and professionals should be aware of.
- Sharing nudes and semi nudes guidance: England - This advice outlines how organisation in England should respond to an incident of nudes and semi-nudes being shared.
- Sharing nudes and semi nudes guidance: Wales - This advice outlines how organisation in Wales should respond to an incident of nudes and semi-nudes being shared.
- SWGfL: Online Safety Policy template - A template which allows schools to create an online safety policy that is relevant to their setting.
- SWGfL: Social Media checklists - Providing simple, practical guidance to help you navigate the safety and privacy features of popular platforms.
- Take It Down - A service for young people to help remove online nude, partially

nude, or sexually explicit photos and videos taken before they were 18.

- Taking photographs: data protection advice for schools - Guidance from the Information Comissioner's Office.
- UKCIS: How to respond to an incident (Overview) - Advice for education settings working with children and young people

About the UK Online Harms Early Warning Working Group

This guidance has been drafted and supported by the following UK Online Harms Early Warning Working Group members:

- Childnet
- Education Scotland
- Embrace (Child Victims of Crime)
- Internet Watch Foundation
- Lucy Faithfull Foundation
- Marie Collins Foundation
- National Crime Agency - CEOP Education
- NSPCC
- Safeguarding Board for Northern Ireland
- Samaritans
- SWGfL
- Tell MAMA
- The Children's Society
- Welsh Government

The UK Online Harms Early Warning Working group is designed to develop early information-sharing between helplines, hotlines, government, law enforcement, and reporting bodies to better identify issues or new trends relating to online harms at an early stage.