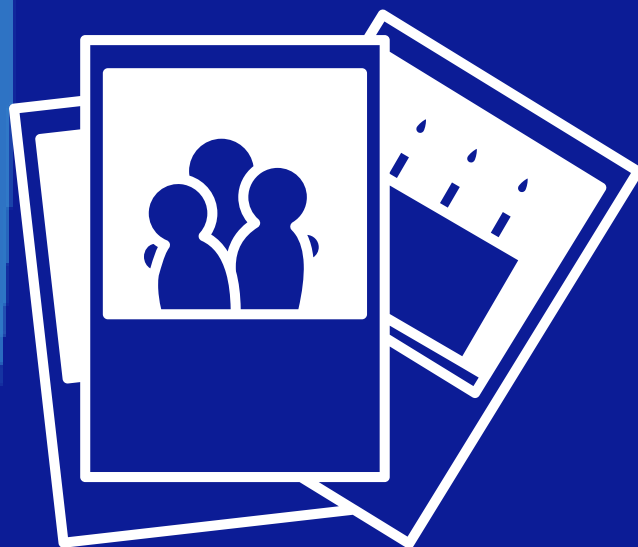




Image Guidance for Schools

Considerations for Protecting Students and Staff



An Roinn Oideachais
agus Oige
Department of Education
and Youth



Co-funded by
the European Union

Table of Contents

Introduction	2
Understanding the risks	3
Considerations for schools	4
Taking photos or videos	5
Publishing photos or videos	7
Responding to incidents	8
Checklist	10
Supports	12

Disclaimer: Information contained in this document does not constitute legal advice. Schools are advised to notify the Gardaí and seek specific legal advice when cases of this nature arise.

About this Guidance

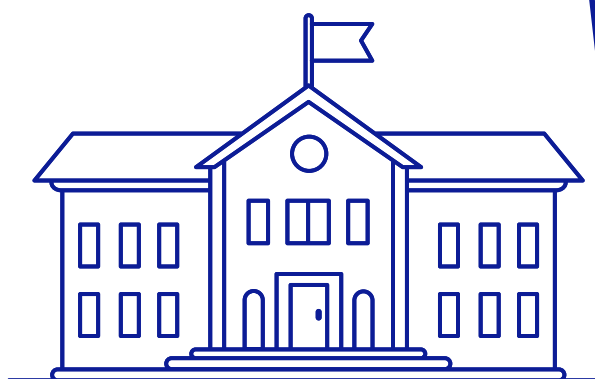
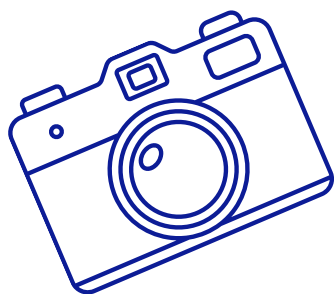
This guidance was developed by Webwise in consultation with the Irish Safer Internet Centre partners (Irish Internet Hotline, ISPCC and National Parents Council) and Oide Technology in Education and is informed by guidance developed by UK Online Harms Early Warning Working Group on [Protecting your setting's images from AI manipulation and abuse](#).



Oide

Technology
in Education

Celebrating students' achievements throughout their time in school is important, and having images of these moments to look back on is a meaningful way of recognising their successes and sharing them with their families. Images and videos can also be used to communicate with parents, promote school activities and record important events. This might include photos and videos taken by staff during classroom activities, performances, and special events, or by staff and volunteers during school trips and off-site activities.



Understanding the Risks

While images and video play a valuable role in school life, there are important safeguarding and child protection considerations to be aware of. Once information is shared online, it can be very difficult to remove, and this may have implications for a child's privacy, safety and digital footprint over time. Developments in AI technology also raise additional concerns, as they can increase the risk of images or videos being manipulated and misused. Schools should therefore be aware of the risks when sharing images online.

Risks of misuse

Images of staff and students can be taken out of context or altered using AI, and there is growing concern about AI being used to create child sexual abuse material (AI-CSAM) or non-consensual images. Shared images can also increase the risk of a child being identified for future grooming or abuse, or being recognised by an existing perpetrator, particularly where a child is already vulnerable. In addition, media reports in the UK indicate criminals have taken student photos from school websites and used AI to create sexually explicit images for a school extortion attempt.

Location safety

Photos can reveal more than intended, including a child's location, school, and routine. Regularly posting this kind of detail can build up a picture of where a child lives and the places they visit, which may pose safety risks.

Digital footprint

Everything shared online contributes to a child's digital footprint, and maintaining a positive online presence is increasingly important as young people grow older. Schools should consider the long-term impact of images shared today. Content that seems harmless now, or even goes viral, may remain publicly accessible and could cause embarrassment or discomfort for the child in later years.

Identity Theft and Impersonation

Images and accompanying information can inadvertently reveal personal details such as birthdays, addresses, or pet names. This kind of information could later be used to support identity fraud, particularly as online scams become more sophisticated. Images or videos could also be used to create impersonation accounts on social media posing concerns and challenges for both staff and students.

Considerations for schools

Schools can reduce the potential for misuse of photos and videos by understanding the associated risks, putting appropriate measures in place, and ensuring that staff and volunteers understand the school's procedures and practices. The considerations below outline key factors to take into account and practical steps schools can take to guide their approach to taking, using and sharing images of students, staff and the wider school community.

Consent

Schools must have up-to-date parental consent for capturing and publishing student images/video/audio. When gaining consent to take photos and videos, it is important to make sure that students and their parents/guardians understand what they are agreeing to, including how long their consent will remain valid, whether consent will be obtained each year or just once, and how they can review or change their preferences during the year.

- Make them aware that photos or videos are being taken
- Explain how images or videos will be used
- Seek written consent from students and parents/guardians before taking or using images
- Explain how long the images will be kept and what will happen when once the retention period has expired
- Explain that consent can be withdrawn, but images that have been used online or in printed material may not be fully removable
- Provide parents, guardians 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 you are 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/carers consent, recognising their growing autonomy and rights, if they are old enough and have the capacity to make their own decisions
- A child may have signed a consent form but that doesn't necessarily mean they want their photograph taken on every occasion. Children and young people should be given the opportunity to assent or decline at the point a photograph or video is being taken. Their decision should be respected without question or consequence.

- Consider involving children and young people, where appropriate, in choosing which images of them are used, particularly where images will be shared publicly. This gives children and young people a sense of control and dignity over how they are represented.
- Where a student or their parent/carer has not given consent for photos or videos, this should be respected, and the student should not be excluded from the activity. Schools should instead make sure anyone taking photos or filming knows who has not consented. Consideration should be given to developing a process to ensure this is managed discreetly and that the child doesn't feel different, identifiable or excluded from their peers.

Taking photos or videos

While it can be safe and appropriate to capture images there are some considerations before taking photos or videos:

- Obtain written consent from parents and students and ensure consent is up to date, informed and covers all purposes and media including social media if used. If images are later being used for a purpose different to the one originally agreed, seek fresh consent or destroy the images
- Be mindful that some children, parents or guardians may not want to have images taken of themselves or their children;
 - Children and families prefer to maintain their privacy
 - Children and families prefer not have an online presence
 - Families have religious or cultural reasons for not wanting photos or videos taken
 - A student with limited or no contact with certain family members may want to minimise their online presence
 - where a student or their family has experienced abuse, they may be concerned that online images could reveal their location to the person responsible
 - a student's identity may need to be protected, for example if they are in local authority care or have been adopted
- Consider the purpose before capturing images, could alternative ways of recording be used for example written records, capturing learner work, etc.
- Be clear on the purpose of any photo or video before taking it
- Only use school owned equipment to take photos or videos, never personal devices, and ensure images are stored securely
- Images should only be taken by an authorised staff member or volunteer with a clear and appropriate reason
- If using a professional photographer, inform parents and students in advance, obtain consent, and give the photographer a clear brief so only students who have consented are included
- Agree in advance how to identify students who have not given consent, without singling them out

School events can be a memorable occasion for all involved, and taking a common-sense and proportionate approach to taking images recognises both the importance of capturing memories and the interests of those involved in the event. For more information on friends and family taking photos at school events, see the Data Protection Commission's blog, [Taking photos at school events – Where common sense comes into play.](#)

What photos or videos to use

Before using or sharing images on the school website, social media or in other publications, schools should carefully consider whether the images are appropriate for the intended purpose and whether they could present any safeguarding or privacy risks. To help minimise potential for misuse or harm schools can consider some key pieces of advice on what type of images to publish (for example; group shots, avoiding close-ups). When capturing or selecting images, schools should consider the following:

- images that present the activity in a positive light and focus on the activity rather than the individual
- where possible, use wider shots that show groups or activities rather than focusing on individual students
- images that capture the activity from a distance rather than close-ups
- where close-ups are necessary, use images that capture students' side on
- where there is no educational or promotional need to identify individual students, consider blurring or obscuring faces
- ensure students are shown in appropriate clothing, including safety wear where relevant
- avoid images that could be more easily misinterpreted or misused
- avoid publishing students' names alongside their image
- avoid publishing personal information about individual students, and disguise any identifying details
- remove location data and other image metadata before uploading ([How to remove metadata from images](#))
- consider reducing image resolution to limit the potential for repurposing

Sharing/publishing photos or videos

Sharing images can be a way of celebrating achievements, showcasing activities, and raising awareness of the school. However, sharing photos or videos through social media or other online platforms has potential risks, for example:

- images may be modified using AI and used inappropriately, for example to blackmail students, families, or school
- photos or videos may appear in online search results, which may make students vulnerable to grooming if an image is shared alongside identifying details such as personal information, a location tag, or visual clues like a school uniform
- once shared online, images can be copied, downloaded, screenshotted, or shared further by anyone
- depending on the platform's terms and conditions, posting an image may give the platform a licence or rights to use the content, which may include sharing or licencing it to third parties, including for commercial purposes
- each image, along with any comments on it, can become part of a student's public profile in ways they may not be comfortable with, now or in the future

Before posting images of students and staff online, schools should also consider how widely the images may be shared, how long they may remain accessible, and what impact this could have on students' long-term wellbeing. Consideration should also be given to which channel is most appropriate for the content being shared. For example, direct email may suit day-to-day class updates, while the website or social media may better suit general achievements intended for a wider audience.

Regularly review photo and video content and platform settings

Schools should carry out regular reviews of the photo and video content published on their website and social media platforms. This includes assessing whether images of students are still necessary, whether older content should be deleted, and considering whether some could be replaced with generic visuals.

Schools should review the privacy and commenting settings (consider turning off comments) on their website and social platforms regularly, to maintain control over who can access and share published images.

Schools should also make efforts to remind parents and students about use of student images and ensure consent is up to date, for example at the beginning of each school year.

Educating Learners

Learners may not be aware of the harm that can be caused by manipulating images or deepfakes of their peers or staff or the legal consequences of generating non-consensual intimate images or AI generated CSAM. Schools can provide students with guidance around AI use through their AUP, their Code of Behaviour and and their Bí Cineálta policy. Relevant policies should be updated to cover AI-manipulated content and the posting of images. Schools should also engage in lessons on consent, rights, reporting and help seeking, cyberbullying, respect and image-sharing using the [Webwise resources](#). Discussions with students should focus on the impact of AI misuse, legal implications and the schools' expectations in relation to AI use.

Responding to Image Misuse Incidents

Schools should consider how they would respond if photographs or videos of students and staff are misused. Depending on the circumstances, this may include:

- preserving evidence of the misuse, where it is safe and lawful to do so. For example, screenshots, messages or links. If in doubt about whether particular content can be lawfully preserved, for example where intimate image abuse (IIH) or child sexual abuse material (CSAM) may be involved, seek guidance from An Garda Síochána before saving or sharing it.
- reporting the content to the relevant online platform and requesting its removal
- informing the Designated Liaison Person (DLP) and following appropriate child protection procedures
- considering whether the matter should be reported to An Garda Síochána or other relevant authorities
- informing affected students and parents/guardians and providing appropriate support
- reviewing whether additional images should be removed from public platforms and whether existing procedures need to be updated.

Some young people will be over 18 whilst still at school 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. The [Irish Internet Hotline](#) can help if an intimate image or video has been shared without consent, they can help with reporting and removing the content online and, in some cases, liaising with An Garda Síochána, should victims wish for it to be investigated by Gardaí.

Good Practice Checklist

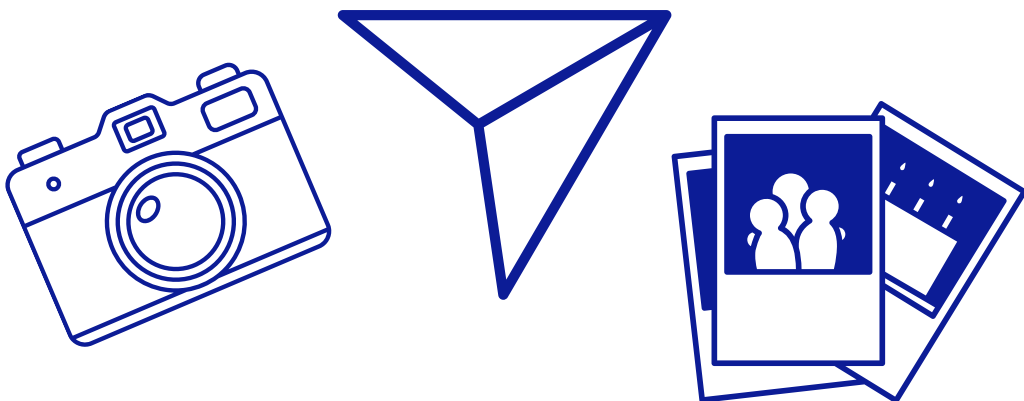
Schools may wish to consider the following before taking, using or sharing images of students:

-  there is a clear purpose for taking or sharing the image
-  appropriate consent has been obtained and is regularly reviewed
-  only school-owned or authorised equipment is being used
-  images are stored securely and access is limited to authorised individuals
-  the image celebrates the activity or achievement rather than focusing on identifying an individual student, wherever possible
-  images have been selected to reduce the likelihood of misuse, for example by using wider shots, side-on photographs, over-the-shoulder images or other images that make students less identifiable where appropriate
-  students' names and other identifying information are not published alongside images unless there is a clear reason for doing so
-  location information, metadata (such as EXIF data) and other unnecessary identifying details have been removed before publication
-  privacy settings on websites, social media platforms and other online services have been reviewed to help limit who can access and share images

- ✓ older images published on websites, social media and promotional materials are reviewed regularly to ensure they remain appropriate in light of evolving AI-related risks
- ✓ staff understand the school's procedures for taking, storing, using and sharing images, including the potential risks associated with AI manipulation
- ✓ the method used to share images is proportionate to the purpose, with the least public option considered where appropriate
- ✓ arrangements are in place to review published images periodically and remove them when they are no longer needed

School photographs can still celebrate important moments but sharing them online requires greater consideration.

An informed approach to publishing images can help protect your school community, reduce the risk of harm, and better prepare schools to respond if issues arise.



Get Support



Part of the Oide Technology in Education, Webwise is the Irish Internet Safety Awareness Centre. Webwise promotes safer, better Internet use through awareness raising and education initiatives targeting teachers, children, young people and parents. Webwise develop and disseminate resources that help teachers integrate digital citizenship and online safety into teaching and learning in their schools. Webwise also provide information, advice, and tools to parents to support their engagement in their children's online lives. Learn more at webwise.ie



The Irish Internet Hotline is the Irish national reporting centre where members of the public can securely, anonymously, and confidentially report concerns in respect of illegal content online, especially child sexual abuse material (CSAM). [hotline.ie/report/](http:// hotline.ie/report/)



ISPCC Childline provides services on a 24/7 basis where children affected by issues encountered on the internet may turn for advice and guidance. Childline can be contacted by any child or young person by calling 1800 66 66 66 or chatting online at Childline.ie



NPC is the national representative organisation for parents. It provides a Helpline and Information Service and Parents' face-to-face and online training courses. Parents can access information at npc.ie or contact the NPC Helpline by calling 01-887 4477

- An Garda Síochána: garda.ie/en/
- Coimisiún na Meán: cnam.ie/general-public/online-safety/
- Data Protection Commission: dataprotection.ie/en

webwise.ie



An Roinn Oideachais
agus Óige
Department of Education
and Youth



Co-funded by
the European Union