

School Photography in the Generative AI Era Guidelines for Schools

'Each generation inherits the task of shaping its own era, of guiding history to become places where the dignity of every person is safeguarded, justice is promoted and fraternity is made possible'

(Pope Leo XIV (2026) in Magnifica humanitas Encyclical Letter on Safeguarding the Human Person in the Time of Artificial Intelligence.)

The rapid growth of accessible generative AI tools has introduced new risks in regards to how photos and videos may be harvested, stored and altered online. AI enabled photo and video manipulation is increasingly realistic and more accessible. Using photos posted by schools to public locations such as social media this technology is being used to create nonconsensual and sexualised images of students and staff. ACS must consider these risks in the context of our duty of care for all our people - our students, our staff and our families. These guidelines serve to ensure our people are 'safe, valued, respected and cared for'.

These guidelines are the first step to move to a model with:

- fewer posts
- clearer purpose
- less identifiable data
- stronger consent
- greater student and staff agency
- tighter image governance
- greater preparedness for AI misuse.

Public Image Sharing

In alignment with guidance from the [eSafety Commissioner](#), schools need to adopt a risk-based approach to help decide which images belong on public channels and which are better shared in closed or restricted spaces.

Schools are only to publicly share photos containing an identifiable individual:

1. **Purpose:** Where the image is moderately necessary for public publication. E.g. promotional and community engagement would not be valid reasons
2. **Consent:** Images shared publicly are to be regularly reviewed to ensure consent remains active.

3. **Identification:** Think about the need to include names, initials or year groups of students at all. Do not use a student's full name.
4. **Old material:** It is recommended that schools are to remove identifiable images of students shared publicly annually.
5. **Low Resolution:** Use of low resolution images lowers the risk of digital manipulation.

Possible ways to share images:

- School newsletter: Newsletters and information shared through Compass and not posted on social media could include more images and details.

Before posting, consider:

- **Purpose:** *What does the image add? Could the same story be told without showing identifiable details?*
- **Consent:** *Is consent active, informed and current? Does it cover school social media posts?*
- **Identification:** *Does the post include a name, uniform, location or routine that could be used to identify a specific person or their location?*
- **Audience:** *Is the account public? Who can view, comment or reshare the content?*
- **Alternatives:** *Are close-ups needed? Could the image be cropped or taken from a distance? Could names be left out?*
- **Settings:** *Are privacy settings and controls for tags or comments reviewed regularly?*
- **Governance:** *Who may post, approve and moderate content? How and where is consent recorded? What processes are in place to review older material?*
- **Old material:** *Do archived pages or past posts still need to remain public?*
- **Storage:** *Are original images stored securely and handled in line with school or sector policies for data retention and disposal?*
(eSafety Toolkit)

Capturing & Framing

Making safer choices for online content doesn't mean shutting down school storytelling all together. Options include:

- Focus on the activity: Action shots from behind, or wider group shots showing learning in progress are engaging while making facial harvesting much harder for automated tools.

- Avoid high-res, tight headshots and crystal-clear, close-up facial portraits publicly. Detailed images are significantly more vulnerable to technical harvesting and AI manipulation.
- Keep student work in the frame: Showcase artwork, science experiments, or group activities where the focus is on the achievement rather than the individual's face.

Examples of how to post and safer images

Capture of digital images, storage and security

The Armidale Catholic Schools Code of Conduct establishes a clear restriction on the use of a worker's personal device to record images in a school setting, including classrooms, sports, and on excursions.

Parental consent for the school to take digital images of a student is given to the school and any decision to undertake and store digital images is a school responsibility which should only be undertaken on a school device and with appropriate, prior approval.

Reporting

In accordance with the Australian eSafety Commissioner, image misuse includes taking, altering, distributing, or threatening to share images or videos of students or staff without their consent. This encompasses image-based abuse (non-consensual sharing of intimate images), AI-generated deepfakes or altered media, unauthorised photography/recording, and cyberbullying using visual content.

If staff become aware of any instance or reasonable suspicion of image misuse, a report must be made immediately to the Principal of the School, School Performance Leader, or the Head of Employee Services of Armidale Catholic Schools.

Support

To support staff with this transition, Tahnee Lowe (Communications and Marketing Coordinator) will be scheduling a Google Meet to discuss practical ways to tell our school stories and craft social posts under these guidelines, this session will cover everyday strategies for creative framing and safer content sharing. Details to join will be shared with Principals & Marketing Liaisons at each school.

As this remains an evolving area of change, we will continue to adapt our practices and policies to be in line with updated advice and legislative changes. This document will be reviewed on a regular basis.