BEHAVIOURAL RISK INTELLIGENCE FOR SCHOOL LEADERSHIP

# Image Guidance for Schools Australia and New Zealand

Protecting students and staff in the age of AI-generated imagery.
This document is guidance, not legal advice. Seek specific legal advice for individual incidents.

## The bottom line

ONE RULE. EVERYTHING FOLLOWS.

**ONE-SENTENCE ANSWER**

Publish only what you would defend in a safeguarding review: Use a data minimisation strategy by using only a small number of consented, low-identifiability images, taken on school-owned devices, stripped of metadata, hosted on a channel you control, reviewed each year, and removed on request.

This is the "so-what" from which every rule below follows. If a proposed image cannot pass the sentence above, do not take it, do not publish it, or take it down.

### Why this matters now

- Big Tech now treats public online images as AI training data by default. Meta scrapes all public Facebook and Instagram posts from Australian adult users to train its AI, with no opt-out offered locally; LinkedIn, X and Google have made similar changes. In parallel, reports of AI-generated child sexual abuse material depicting real students have risen sharply across Australia and New Zealand. Assume any face posted publicly  student, staff or parent can be harvested and reused.

- School websites and public social feeds are the highest-yield source of student images for offenders and extortion rings, because they are indexed, uniformed, tagged with names, and rarely reviewed.

- Your existing obligations already require this level of care.
  **In Australia:** the Privacy Act 1988, the National Principles for Child Safe Organisations, the Online Safety Act 2021, and state Reportable Conduct Schemes.
  **In New Zealand:** the Privacy Act 2020, the Children's Act 2014, the Harmful Digital Communications Act 2015, and the Films, Videos, and Publications Classification Act 1993.

- Both countries are now legislating on minimum age and platform duty. Australia's under-16 restriction is in force. New Zealand's Online Safety (Minimum Age and Child Safety Risk Assessment) Bill was introduced on 24 August 2026 and would require platforms to risk-assess harms to children, including AI-generated deceptive content. Schools that tighten image practice now will be ahead.

## Situation and complication

### Situation

Schools capture student and staff images every week: assemblies, sport, drama, excursions, camps, graduations, marketing shots. Families expect to see these moments. Schools use them to celebrate, communicate, and enrol.

### Complication

- Generative AI has made it trivial to strip clothing, swap faces, or fabricate sexual imagery from a single ordinary school photo, often within seconds and on free consumer apps.
- There are documented overseas (UK) cases of criminals lifting student photos from school websites and using AI to build sexually explicit images for extortion attempts against the school and the child.
- Once an image is public you cannot recall it. It is copied, cached, scraped, and licensed onward by the platform under its own terms.
- Consent given once at enrolment does not survive a technology change of this magnitude. Families increasingly want granular, revocable, informed consent, and both the Australian and New Zealand privacy regulators have said so in guidance.

### Question this document answers

*How should the school capture, select, publish, review, and respond to incidents involving student and staff images, given AI risk and current law in Australia and New Zealand?*

### How to read this document

The answer sits at the top, and each supporting section explains one reason it is correct. You can read only the boxes and headings and still act correctly. Sections 1 to 8 apply in both countries. Sections 9 and 10 are the jurisdiction-specific anchors.

| SECTION | WHAT IT GIVES YOU |
|---|---|
| **1. Bottom line** | The one-sentence rule the school follows |
| **2. Situation and complication** | Why the old approach is no longer safe |
| **3. Six operating principles** | The reasons behind the rule. Memorise these |
| **4. Before you take an image** | Capture checklist |
| **5. Before you publish an image** | Publishing checklist |
| **6. Ongoing review** | What you do every year, without fail |
| **7. When something goes wrong** | Incident response and reporting lines for both countries |
| **8. Roles and accountability** | Who owns what |
| **9. Legal map, Australia** | Australian statutory anchors |
| **10. Legal map, New Zealand** | New Zealand statutory anchors |
| **11. One-page checklist** | Print, laminate, distribute |
| **12. Family-facing summary** | Paste into your newsletter or handbook |

## Six operating principles

The rest of this document is these six ideas restated in operational language.

01 CONSENT

Blanket "yes to all photos, forever" consent no longer meets community expectations or contemporary privacy law in either country. Split consent by channel: internal use, school website, social media, external media. Refresh at least annually. Honour withdrawal, including for images already published, to the extent removal is technically possible. New Zealand schools should note that the Privacy Commissioner's 2025 photography and filming guidance treats purpose limitation strictly. An image collected for one purpose cannot quietly become marketing material.

**Blanket yes-to-everything-forever is no longer defensible.**

02 THE CHILD

**The in-the-moment no outranks the yes**

A signed form is a permission, not a compulsion. A student who declines on the day must never be photographed, singled out, or excluded from the activity. Where a young person is old enough to form a view, that view is part of the consent, not a courtesy.

**The child's no is not a negotiation.**

03 DEVICE

### Capture on school-owned devices only

Personal phones create untraceable copies, retain location metadata, and expose staff. Use only school-managed cameras or devices, with images stored in school-managed cloud storage under role-based access. If a personal device is ever unavoidable, the image is transferred to school storage and deleted from the device the same day, and that exception is logged.

**If the device is not the school's, the image is not controlled.**

04 FRAMING

### Reduce identifiability by default

Wider shots over close-ups. Activity over face. Side-on where a close-up is unavoidable. No names next to faces. Never combine uniform, location and name in the same post. Blur or exclude where there is no educational purpose in identifying the child. Remember that identifiability is not only the face: a distinctive wheelchair, a name on a jersey, or a recognisable school gate will do the same work for an offender.

**Frame for what they did, not for who they are.**

05 PREPARATION

### Strip metadata and downscale before publishing

Remove EXIF data, including GPS, device and timestamp, and reduce resolution before any public post. High-resolution originals stay internal. Low-resolution, metadata-stripped copies go public. This is explicit advice from the New Zealand Privacy Commissioner and sits inside Australian Privacy Principle 11 on security.

**High-resolution originals stay internal. Always.**

06 CHANNEL

## Least-public channel that achieves the purpose

Direct email or a parent portal for class updates. Website and public social for celebratory community moments only. Prefer channels where you control access, retention, and takedown. Ask what licence you grant the platform by checking terms every time you post and review those terms annually.

**Control the channel, or you control nothing that follows.**

## Before you take an image

**ASK, IN ORDER:**

1. Is there a defensible purpose that written work, a wide shot, or an anonymised alternative cannot serve?
2. Is current, informed, channel-specific consent in place for every student in the frame?
3. Has anyone in the frame indicated, verbally or through body language, that they do not want to be photographed today?
4. Am I using a school-owned, school-managed device with secure storage?
5. Have I framed for activity, not identity: wide, side-on, or over-the-shoulder where possible?
6. Do I know how images of non-consenting students will be handled discreetly, without singling them out?

### If a professional photographer is used

- Notify parents and students in advance and re-obtain consent for that shoot.
- Give the photographer a written brief: purpose, permitted uses, non-consent list, storage handover, deletion timeline.
- Contract requires the photographer to hand over all files, delete their own copies, and not use images in their portfolio.
- Agree a discreet method for identifying non-consenting students in advance: coloured wristbands, name lists held by the class teacher, never a public callout.
- In New Zealand, confirm the photographer is safety-checked where the engagement makes them a children's worker under the Children's Act 2014. In Australia, confirm a current Working with Children Check or state equivalent.

### Situations where extra care is required

- Students in out-of-home care, foster care, or with restricted-contact orders.
- Students from families experiencing family violence, coercive control, or witness protection.
- Adopted students, and whāngai placements, where identity protection has been requested.
- Students with cultural or religious reasons to avoid image capture. For Māori and Pacific families this can include images connected to whakapapa, images taken at a marae or during tangihanga, and the ongoing use of images of a student who has died. Ask, do not assume, and follow the whānau lead.
- Students whose family has asked to minimise online presence for any reason. The reason does not need to be justified.

## Before you publish an image

**THE PUBLISHING TEST**

If the image were downloaded, deepfaked, geolocated by uniform and background, and re-posted with the student's name, would the school still be comfortable it was published?
If no, do not publish.

### Selection

- Activity in focus, not the individual.
- Wide or group shot preferred. Close-ups only where educationally necessary and captured side-on.
- No safety concerns visible: unsafe practice, missing protective equipment, exposed lanyards with full names.
- No visible location markers combined with uniform or timetable clues.

### Preparation

- EXIF and other metadata stripped: GPS, device, timestamp, author.
- Resolution reduced to what the channel needs, typically 1200 px on the long edge for web, less for thumbnails.
- Filename anonymised. No student name, class code, or date pattern.
- No student name in caption, alt text, or file metadata unless there is a specific consented reason.

### Channel

- Least-public channel that serves the purpose. Prefer parent portal or direct email over public feeds.
- Comments turned off on any public post carrying student images.
- Public social channels reviewed annually for platform terms. What licence does posting grant the platform?

### Record

- Log the image, its purpose, the consent status of every identifiable person, the channel, the publish date, and the planned takedown date.
- Rolling annual audit: is this still needed, still consented, still appropriate?

## Ongoing review

- Annual review of all public image content on the school website, social channels, and printed marketing. Delete anything without ongoing purpose, consent, or accuracy.
- Annual re-consent cycle, communicated to families in the first fortnight of the school year.
- Platform-settings audit: privacy controls, commenting, tagging, sharing permissions. Comments off by default on posts featuring students.
- Staff refresh: annual short training module and signed acknowledgement.
- Register of image incidents, near-misses, and takedown requests. Trend review each term.
- New Zealand boards should fold this review into the three-yearly child protection policy review required by the Children's Act 2014, and not wait three years to do the image audit.

## When something goes wrong

**DO THIS FIRST, IN THIS ORDER**

1. Protect the child. Check on the student and family. If a criminal offence is possible, do not view, forward, download, or store the material yourself.

2. Notify. Escalate immediately to the designated safeguarding role and your school leader.

3. Preserve evidence lawfully. Screenshots or URLs where lawful. Where child sexual abuse material or intimate-image abuse may be involved, do not save the material. Record the URL and time and let police and regulators direct evidence handling.

4. Report to authorities. See the reporting lines for your country below.

5. Report to the platform and request takedown.

6. Support the student and family. Dedicated staff contact, wellbeing support, and a communications plan.

7. Review. What changed the risk? What image, channel, or process needs to change permanently?

### Reporting lines, Australia

- For any suspected criminal offence, including AI-generated child sexual abuse material, image-based abuse, sextortion, or threats involving a child under 18yrs Australian Centre to Counter Child Exploitation www.accce.gov.au
- Image-based abuse and illegal content www.esafety.gov.au/report eSafety can compel removal of image-based abuse under the Online Safety Act 2021 within short statutory timeframes.
- State Reportable Conduct Scheme, being the NSW Office of the Children's Guardian, the Victorian Commission for Children and Young People, or the equivalent state or territory regulator, where a staff member or volunteer is implicated in image misuse involving a child.
- Office of the Australian Information Commissioner for eligible data breaches involving personal information under the Notifiable Data Breaches scheme: oaic.gov.au.
- Kids Helpline 1800 55 1800 and Lifeline 13 11 14 for student and family wellbeing support.
- Safe on Social powered by Ctrl+Shft www.safeonsocial.com – Community Connect education resources and 24/7 support

## Reporting lines, New Zealand

- New Zealand Police for any suspected criminal offence. Emergency 111, non-emergency 105. This includes AI-generated child sexual abuse material, intimate visual recordings, sextortion, and threats.
- Department of Internal Affairs, Digital Child Exploitation Team, for objectionable material including AI-generated and fully synthetic child sexual abuse material: dia.govt.nz. DIA is the enforcement agency, not the Police, for censorship offences.
- Netsafe, the approved agency under the Harmful Digital Communications Act 2015, for harmful digital communications, image-based abuse, and takedown assistance: 0508 638 723, help@netsafe.org.nz, or text "Netsafe" to 4282. Netsafe assesses and investigates complaints and can escalate to the District Court for removal orders.
- Oranga Tamariki on 0508 326 459 for a report of concern where a child's safety is at risk, alongside Police.
- Teaching Council of Aotearoa New Zealand, where a teacher may have committed serious misconduct. Section 491 of the Education and Training Act 2020 makes that report mandatory for the employer.
- Office of the Privacy Commissioner via NotifyUs, where a privacy breach is likely to cause serious harm. The Privacy Act 2020 requires notification as soon as practicable, and the regulator treats 72 hours as the working benchmark: privacy.org.nz.
- 1737 free call or text, and Youthline 0800 376 633, for student and family wellbeing support.
- Safe on Social powered by Ctrl+Shft www.safeonsocial.com – Community Connect education resources and 24/7 support

## Common pitfalls to avoid, both countries

- Staff or the designated safeguarding lead viewing, forwarding, or downloading the image "to see how bad it is". This can itself be a criminal offence.
- Deleting evidence before authorities have advised on preservation.
- Communicating with the perpetrator directly instead of via police.
- Treating an AI-generated fabricated image as "not real" and therefore not a safeguarding matter. It is a safeguarding matter, and in both countries it is very likely a criminal one.
- Failing to notify affected students and parents on the assumption that less said is better.
- Assuming an Australian process works in New Zealand. There is no eSafety Commissioner in New Zealand and no Reportable Conduct Scheme. The equivalents are Netsafe, DIA, and the Teaching Council.

## Roles and accountability

A rule without a named owner is a rule that lapses. Assign every row of the following table to a named individual and review at least annually.

| ROLE | OWNERSHIP |
|---|---|
| **Principal, Tumuaki or Head of School** | Owns this policy, signs off on the annual review, and is the final decision-maker on incidents. |
| **Child Safety Officer or Child Protection Lead** | Primary escalation point for suspected image misuse involving a child. Liaison to Police, and to eSafety and the Reportable Conduct regulator in Australia, or Netsafe, DIA and Oranga Tamariki in New Zealand. |
| **Deputy or Business Manager** | Owns the consent register, the image inventory, and the annual audit of published content. |
| **Communications or Marketing Lead** | Owns the publishing workflow, channel selection, metadata stripping, comments-off enforcement, and takedown execution. |
| **ICT or Digital Lead** | Owns device management on school-owned devices only, storage security, access control, and network filtering that blocks nudify apps and deepfake generators. |
| **Classroom teachers and coaches** | Own in-the-moment consent, meaning the student "no today", safe framing, and correct device use. |
| **Board or governing body** | Approves the policy and receives an annual report on image incidents, near-misses, and takedowns. In New Zealand this sits with the school board alongside the three-yearly child protection policy review. |

## Legal and regulatory map, Australia

COMMONWEALTH AND STATE ANCHORS.

| INSTRUMENT | WHAT IT REQUIRES OF SCHOOLS |
|---|---|
| **Privacy Act 1988 (Cth) and the Australian Privacy Principles** | Collect only what is necessary (APP 3), give notice at collection (APP 5), use only for the notified purpose (APP 6), and secure and dispose of images (APP 11). A student photograph is personal information. A photo tied to name, class, or health information is sensitive information and requires stronger consent. |
| **Online Safety Act 2021** | eSafety can order the removal of image-based abuse and cyberbullying material targeting an Australian child within short statutory timeframes of a valid notice. Australian Centre to Counter Child Exploitation for images of a child under 18yrs. |
| **Criminal Code Act 1995 (Cth) and state equivalents** | AI-generated child sexual abuse material is child abuse material. Producing, possessing, or transmitting it is a criminal offence, regardless of whether the depicted person exists. |
| **National Principles for Child Safe Organisations** | Principle 1 on child safety as a strategic priority, Principle 3 on family and community involvement, Principle 8 on staff knowledge and skills, and Principle 10 on continuous improvement. |
| **State Reportable Conduct Schemes** | Certain conduct by staff or volunteers involving a child, including sexual misconduct via images, is reportable to the state regulator in addition to police. |
| **Child Safe Standards** | Standards 1, 2, 3 and 8 explicitly cover online safety and image handling. |

This document is guidance, not legal advice. Seek specific legal advice for individual incidents.

## Legal and regulatory map, New Zealand

| INSTRUMENT | WHAT IT REQUIRES OF SCHOOLS |
|---|---|
| **Privacy Act 2020 and the Information Privacy Principles** | Collect only for a lawful purpose connected to your functions (IPP 1), collect directly and fairly (IPP 2 and 4), tell people why you are collecting (IPP 3 and 3A), keep images secure (IPP 5), do not keep them longer than needed (IPP 9), and do not use or disclose them beyond the notified purpose (IPP 10 and 11). A student photograph is personal information. |
| **Privacy Act 2020, notifiable privacy breach scheme** | A privacy breach likely to cause serious harm must be notified to the Office of the Privacy Commissioner and to affected individuals as soon as practicable. The regulator treats 72 hours as the working benchmark. A leaked image set is a notifiable breach. |
| **Privacy Commissioner photography and filming guidance (2025)** | Consent must be informed and can be withdrawn. Images collected for one purpose must not be repurposed. Avoid personal devices. Remove embedded metadata before publishing. The guidance expressly warns that misappropriated images can be edited into child sexual abuse material using AI. |
| **Harmful Digital Communications Act 2015** | Sets ten communication principles and creates offences for posting a harmful digital communication and for posting an intimate visual recording without consent. Netsafe is the approved agency for complaints, and the District Court can order removal. |
| **Films, Videos, and Publications Classification Act 1993** | Child sexual abuse material is objectionable whether it is real, AI-generated, or fully synthetic. Possession and distribution are serious criminal offences. The Department of Internal Affairs enforces this. |
| **Crimes Act 1961, sections 216G to 216N** | Making, possessing, publishing, or distributing an intimate visual recording without consent is a criminal offence, separate from the censorship regime. |
| **Children's Act 2014** | School boards must have a written child protection policy that sets out how suspected abuse and neglect are identified and reported, reviewed at least every three years, and must safety-check children's workers. |
| **Education and Training Act 2020** | Boards must take all reasonable steps to ensure the physical and emotional safety of students. Section 491 makes reporting possible serious misconduct by a teacher to the Teaching Council mandatory for the employer. |
| **Online Safety (Minimum Age and Child Safety Risk Assessment) Bill** | Introduced 24 August 2026, not yet law. Would require platforms to take reasonable steps to keep under-16s off accounts and to publish child safety risk assessments covering grooming, self-harm material, and AI-generated deceptive content. Worth tracking, not yet compliance. |

This document is guidance, not legal advice. Seek specific legal advice for individual incidents.

## One-page checklist

PRINT. LAMINATE. DISTRIBUTE.

Print, laminate, and distribute to every classroom, sports staff room, and reception.

### BEFORE YOU TAKE AN IMAGE

- Purpose is clear and cannot be met by a lower-risk alternative.
- Consent is current, informed, and channel-specific.
- No student in frame has indicated they do not want to be photographed today.
- School-owned device, secure storage.
- Framing minimises identifiability.

### BEFORE YOU PUBLISH AN IMAGE

- Wider shot, activity over face, no unsafe scenes.
- No student name paired with face. No location and uniform combination.
- Metadata stripped, resolution reduced, filename anonymised.
- Least-public channel that serves the purpose.
- Comments off, annual takedown date logged.

### IF MISUSE IS SUSPECTED

- Do not view, download, or forward suspected illegal material.
- Escalate immediately to the designated safeguarding role.
- Australia: Police, ACCCE, eSafety, Reportable Conduct Scheme, OAIC if data was breached.
- New Zealand: Police, DIA, Netsafe, Oranga Tamariki, Teaching Council, Privacy Commissioner if data was breached.
- Support the child and family. Document everything.

## Family-facing summary

SAY IT PLAINLY TO FAMILIES.

Paste this into your school newsletter, family handbook, or enrolment pack.

**FOR FAMILIES**

We celebrate your child's achievements in ways that also protect their long-term privacy. Photos and video are only ever taken with a defensible reason, on school-owned devices, by staff who have signed our image policy. We prefer wider shots over close-ups, and we never publish your child's name alongside their photo.

You control what you consent to, and you can change your mind at any time. Every year we ask you to review your image preferences. Internal use, the school website, social media, and external media each get their own tick box.

If your child says "not today" on the day of an activity, we respect that without question or consequence, even if you have signed the annual consent form.

If your family has cultural reasons for limiting images of your child, please tell us. We will follow your lead, and we will not ask you to justify it.

AI has made it easy to alter or fabricate images of children. That is why we strip location data, reduce image resolution before publishing, review our public channels every year, and delete images that no longer serve a purpose.

If you are ever concerned about an image of your child online, tell us.

We will investigate, take it down where we can, and support your family through any report to authorities.

## Sources and further reading

PRIMARY SOURCES ONLY.

### Australia

- eSafety Commissioner: www.esafety.gov.au
- Australian Human Rights Commission: National Principles for Child Safe Organisations, www.childsafe.humanrights.gov.au/national-principles
- Office of the Australian Information Commissioner: Australian Privacy Principles guidelines, www.oaic.gov.au/privacy/australian-privacy-principles

### New Zealand

- Office of the Privacy Commissioner: Children and young people, photography and filming guidance (2025), www.privacy.org.nz
- Office of the Privacy Commissioner: Children's privacy guidance for the education sector, and NotifyUs breach reporting, www.privacy.org.nz
- Netsafe: Harmful Digital Communications Act helpline and guidance on child sexual abuse material, www.netsafe.org.nz
- Department of Internal Affairs: Digital Child Exploitation Team, reporting objectionable material, www.dia.govt.nz
- Ministry of Education: school child protection policy requirements under the Children's Act 2014, www.education.govt.nz
- Teaching Council of Aotearoa New Zealand: mandatory reporting of possible serious misconduct under section 491.

*Prepared by Kirra Pendergast, Founder, Chief Intelligence Architect*
*Safe on Social and Ctrl+Shft*
*www.safeonsocial.com*
*Guidance only, not legal advice. All rights reserved © 2026*