

FREE OWNER'S GUIDE · 2026 EDITION

CCTV in Australian Childcare

What the 2025–26 child safety reforms mean for your cameras, your families and your staff, and how to get CCTV right.

For approved providers, owners, nominated supervisors and centre directors

Current as at October 2026 · Published by GreeneDesk Pty Ltd

In this guide

1. At a glance: what changed and when
2. Is CCTV mandatory in childcare?
3. The national CCTV assessment
4. Your legal obligations
5. Where cameras can and cannot go
6. Telling families and staff
7. Storage, access and retention
8. Why recording is not supervision
9. CCTV readiness checklist
10. Questions to ask any CCTV or AI vendor

1. At a glance

Since mid-2025, child safety in early childhood education and care (ECEC) has been reshaped by national reforms agreed by all Education Ministers. CCTV has moved from "nice to have" to something families ask about at enrolment and regulators expect to be governed properly. These are the changes that matter most for cameras and devices.

Date	What changed	Why it matters for CCTV
1 Sep 2025	Services must have policies and procedures for the safe use of digital technologies, including parental consent, and for any optical surveillance device (e.g. CCTV) they intend to use (regulation 168).	If you run CCTV, a written CCTV policy is now a regulatory requirement, not best practice.
1 Sep 2025	Physical or sexual abuse allegations must be notified to the regulatory authority within 24 hours (previously 7 days).	You need to be able to find and preserve relevant footage fast.
1 Jan 2026	National Quality Standard refined: Element 2.2.3 becomes Child Safety and Protection; Standard 7.1 and Element 7.1.2 now refer to a child safe service and risk management.	Assessors look at how your systems, including CCTV governance, support a child safe culture.
2 Jan 2026	Maximum penalties under the National Law increased and more offences became infringement offences.	Gaps in policy and practice cost more.
27 Feb 2026	Personal devices banned while working directly with children in centre-based services (with limited exceptions); only service-supplied devices may capture, store or transmit images of children. Mandatory child safety training. No new service waivers for regulation 115 (premises designed to facilitate supervision).	Authorised CCTV is treated differently from personal devices (see section 4). Blind spots must be designed out, not waived.
Apr–Jun 2026	National CCTV assessment data collection in up to 300 services.	Nationally consistent best-practice guidance on CCTV is expected to follow.

Sources: ACECQA, Progress on Child Safety review recommendations (April 2026); ACECQA information sheet, Using digital devices in centre-based education and care services; Department of Education, National CCTV assessment.

2. Is CCTV mandatory in childcare?

Generally, no. As at October 2026 there is no national law requiring every centre to install CCTV. The Australian Government has said the national CCTV assessment is not about laying the foundations for a national rollout.

However, three things mean many services are installing it anyway:

- **Conditions on service approval.** Some regulatory authorities have placed conditions on individual services requiring CCTV in key indoor and outdoor areas, with policies on use, security and access. Check your own service approval on the ACECQA national register.
- **Provider decisions.** Several large operators publicly committed in 2025 to CCTV across all their centres, which has shifted family expectations.
- **Family demand.** Parents increasingly ask "Do you have cameras?" at enrolment tours. A clear, well-governed answer is now part of how centres win trust.

The practical position

If you already have CCTV, the law requires you to govern it (policy, notice, secure storage, timely access for authorised officers). If you are considering CCTV, plan the governance before the install, not after.

3. The national CCTV assessment

In August 2025, Education Ministers commissioned a national assessment of CCTV in ECEC. Key facts:

- Up to **300 services** nationally, across service types and including regional, rural and remote communities.
- Designed and delivered by Nous Group for all governments, overseen with the Australian Centre for Child Protection, with an expert panel including the AFP, the Office of the Australian Information Commissioner, the National Office for Child Safety and ACECQA.
- Data was collected from **April to June 2026**. The assessment has concluded, with a final report to Education Ministers due in the third quarter of 2026.
- Its purpose is an evidence base for **nationally consistent best-practice guidelines**, including privacy, data storage, footage retention and day-to-day operation.
- The Government notes there are few studies on whether CCTV prevents harm or helps investigations, which is why it is being assessed carefully.

What to do now: build your CCTV practice on the principles the assessment is testing (ethics, safety, transparency, privacy and secure storage) so you are ready when national guidance is published.

4. Your legal obligations

National Law and Regulations

- **Regulation 168 policy.** If you use CCTV, have a written policy and procedure that informs families about the CCTV and its purpose (and seeks the permissions you need), explains how footage is stored, secured and accessed, and ensures timely access to footage for authorised officers and others such as police when requested.
- **Personal device rules do not cover authorised CCTV.** From 27 February 2026, the offences for capturing, storing or transmitting images of children on unauthorised devices do not apply to images captured by an optical surveillance device (such as CCTV) installed at the service premises and authorised by the approved provider. That exemption depends on the system being installed at your premises and authorised by you. Viewing or copying footage onto personal phones is a different matter and should be prohibited in your policy.
- **Regulation 115 and supervision.** Premises must be designed and maintained to facilitate supervision at all times. CCTV can support this but does not replace good design, positioning and active supervision.
- **Record keeping.** Footage that forms part of an incident, injury or allegation record must be kept in line with the record-keeping rules (incident records are generally kept until the child turns 25). ACECQA's record-keeping guidance reflects the Royal Commission recommendation that records relating to child sexual abuse allegations be kept for at least 45 years.

Privacy law

- The **Privacy Act 1988** and the **Australian Privacy Principles (APPs)** govern how identifiable footage is collected, used, stored and disclosed. Many providers are covered; even if your business is exempt, the APPs are the benchmark regulators and families will hold you to.

- The Office of the Australian Information Commissioner is developing a **Children's Online Privacy Code** that will set clearer expectations about children's personal information.

State and territory surveillance and workplace laws

Surveillance device and workplace surveillance laws vary by jurisdiction. They mainly affect **audio recording, notice to staff** and **private areas**. A summary to discuss with your adviser:

Jurisdiction	Key laws to check	Practical notes
NSW	Workplace Surveillance Act 2005; Surveillance Devices Act 2007	Written notice to employees at least 14 days before camera surveillance starts; cameras visible; signs at entrances.
ACT	Workplace Privacy Act 2011	Similar 14-day notice and signage requirements for workplace surveillance.
VIC	Surveillance Devices Act 1999	Optical surveillance of private activities without consent is restricted; surveillance in workplace toilets, washrooms and change rooms is prohibited.
SA	Surveillance Devices Act 2016	Restrictions on recording private activities and conversations; disclose cameras to guardians and staff.
WA	Surveillance Devices Act 1998	Restrictions on recording private activities and conversations; WA has its own National Law commencement dates.
QLD	Invasion of Privacy Act 1971	Mainly governs listening devices (audio).
TAS	Listening Devices Act 1991	Mainly governs audio recording.
NT	Surveillance Devices Act 2007	Restrictions on recording private activities and conversations.

Simple rule that keeps you safe in every state

Do not record audio, keep cameras out of private areas, tell staff and families in writing before cameras go live, and put up clear signs.

5. Where cameras can and cannot go

Usually appropriate	Never appropriate
Play rooms and learning spaces	Toilets and bathrooms
Outdoor play areas, fence lines and gates	Nappy change areas
Entries, exits and the pickup point	Change rooms (children or staff)
Corridors and transition spaces	Staff toilets and private rest areas
Sleep rooms, with a clear purpose and policy, positioned to show supervision rather than children in a state of undress	Anywhere children's privacy and dignity would reasonably be expected
Kitchens and storerooms (for hazard and access control)	

Position cameras to show **supervision and sight lines** (where educators are, where children are, entries and blind spots) rather than close-ups of individuals. Review coverage against your supervision plan: every blind spot your educators struggle to see should be either designed out or covered.

6. Telling families and staff

Transparency is the foundation of a defensible CCTV program. Before cameras go live (or now, if they are already running):

1. Update your **enrolment agreement and privacy notice** to describe the CCTV, its purpose, where cameras are, who can view footage and how long it is kept.
2. Give **staff written notice** (at least 14 days in NSW and the ACT) and consult them. Make clear CCTV is for child safety and is not used for routine performance monitoring.
3. Put **signs at every entrance** stating that CCTV operates on the premises.
4. Publish a short **CCTV policy summary** families can read, and explain how they can raise concerns.

Sample notice paragraph (adapt with your adviser)

"[Service name] uses closed-circuit television (CCTV) in play areas, outdoor areas, entries and corridors to support the safety and supervision of children. Cameras are not placed in toilets, nappy change or change areas, and no audio is recorded. Footage is stored securely on site and in Australia, viewed only by authorised staff for safety, incident and compliance purposes, provided to regulatory officers or police when lawfully requested, and deleted after [X] days unless needed for an incident or investigation. Our full CCTV policy is available on request."

7. Storage, access and retention

Area	Good practice
Where footage lives	On site or in Australian-hosted storage. Avoid systems that stream or store identifiable footage overseas.
Who can view	A named, short list (approved provider, nominated supervisor, delegated director). Live viewing for supervision purposes only.
Access log	Record every review, export and disclosure: who, when, why and what was provided.
Exports	Only to encrypted service media for a documented purpose. Never onto personal phones.
Retention	There is no single national period yet. Many services keep routine footage 14–30 days. Preserve footage linked to incidents, complaints or allegations immediately, and keep it with the incident record.
Requests	A clear process for regulatory authorised officers and police (timely access is required) and for families' requests under privacy law.
Cybersecurity	Change default passwords, use multi-factor authentication, keep firmware updated, put cameras on a separate network, and restrict remote access.
Audio	Off.

8. Why recording is not supervision

Traditional CCTV is **passive**. It records footage nobody is watching, and it is reviewed after something has already gone wrong. In a busy centre, no director can watch 10–30 camera feeds while running the service.

That leaves the gap the reforms are aimed at: the moments between headcounts, during transitions, at the back of the yard or when a personal phone comes out. Those moments are what assessors probe under Element 2.2.1 (Supervision) and what families fear most.

Recording-only CCTV	CCTV with AI supervision alerts
Footage reviewed after an incident	Alerts educators while there is still time to act
Blind spots go unnoticed for hours	Flags a child alone in a zone, a gate left open, a child near a fence
No evidence that supervision happened	Timestamped alert and response records for QA2 and QA7 evidence
Phone use found only by chance	Flags personal phones in children's areas, supporting the device ban
Hours of manual review to find one event	Events are already logged and searchable

AI alerts support, and never replace, active supervision by educators. Choose a system that processes video on site, does not identify people on CCTV and blurs faces in alerts, so the safety benefit does not come at the cost of privacy.

9. CCTV readiness checklist

Tick each item. Anything unticked is a gap to close before your next assessment and rating visit.

Governance

- ☐ Written CCTV policy and procedure under regulation 168, approved and dated
- ☐ Purpose of CCTV is stated (child safety, supervision, incident response)
- ☐ Named people authorised to view, export and disclose footage
- ☐ Process for timely access by authorised officers and police
- ☐ Policy reviewed at least annually and after any incident

Families and staff

- ☐ Enrolment agreement and privacy notice updated
- ☐ Staff given written notice and consulted (14 days in NSW and ACT)
- ☐ Signs at all entrances
- ☐ Staff trained on the CCTV policy and the personal device rules

Cameras and coverage

- ☐ No cameras in toilets, nappy change, change rooms or staff private areas
- ☐ No audio recording
- ☐ Coverage mapped against the supervision plan and known blind spots
- ☐ Entries, gates, fence lines and the pickup point covered

Storage and security

- ☐ Footage stored on site or in Australia
- ☐ Default passwords changed, MFA on, firmware current, cameras on a separate network
- ☐ Access log in place for every view, export and disclosure
- ☐ Retention period set, with a hold process for incidents and allegations
- ☐ No footage on personal devices

Supervision

- ☐ CCTV complements active supervision, positioning and headcounts, and is never a substitute
- ☐ Considered live alerting so risks are caught as they happen, not only reviewed afterwards

10. Questions to ask any CCTV or AI vendor

Question	What a good answer looks like
Where is video processed and stored?	On site, or in Australia. No identifiable footage sent overseas.
Does it recognise or identify people on CCTV?	For supervision, it should not need to. Look for face recognition switched off on CCTV and faces blurred in alerts.
Does it work with my existing cameras?	Works with standard IP cameras and recorders, after a coverage review.
What does it actually alert on?	A clear list of configured safety events, not vague promises.
How fast are alerts and who receives them?	Seconds, to the nominated educator or supervisor's phone or tablet.
How are false alerts handled?	Configurable zones and thresholds, with tuning after go-live.
Is it used to monitor educator performance?	It should be a safety-event system, not a staff scoring tool.
What records does it keep for QA2 and QA7?	Timestamped alert and response logs you can export for assessors.
What security certification does the platform hold?	ISO 27001 or equivalent, plus Australian data hosting.
Who supports me locally and what does it cost?	An Australian support line and a clear per-centre price.

About SooperVision

SooperVision is AI supervision software for Australian childcare centres, delivered by GreeneDesk Pty Ltd (ABN 13 958 181 688) and powered by FaceTagr. It runs on a centre's existing CCTV and alerts educators to configured supervision risks such as a child alone in a zone, a ratio drifting, a gate left open or a personal phone in a children's area.

Video is processed on-site. CCTV supervision does not recognise or identify anyone; face recognition is switched off on CCTV and faces are blurred in alert snapshots. Optional, separate modules use consent-based face verification for authorised pickup adults and educator attendance. Children are never enrolled or identified.

Pricing from A\$350 per centre per month. **soopervision.com.au** · **1300 181 665** · **anita.w@greenedesk.com**

Sources

[ACECQA: Progress on Child Safety review recommendations \(April 2026\)](#)

[ACECQA: Using digital devices in centre-based education and care services](#)

[ACECQA: NQF child safety changes from 1 September 2025 and 1 January 2026](#)

[Department of Education: National CCTV assessment](#)

[Department of Education: Joint action on child safety in ECEC](#)

[Office of the Australian Information Commissioner: Australian Privacy Principles](#)

This resource is general information for Australian education and care services, current as at October 2026. It is not legal advice. Laws differ between states and territories (NSW applies its own version of the National Law, and Western Australia has its own commencement dates). Check current requirements with your regulatory authority and get legal advice for your circumstances.