GOVERNANCE & COMMUNICATIONS:

Social Media Policy

PURPOSE

This policy provides clear guidelines on the responsible and appropriate use of social media by our education and care service, its educators, staff, volunteers and students on placement. It applies to both official service social media accounts and personal social media use where that use relates to the service, its children, families or colleagues.

Our service is committed to:

- Protecting the safety, privacy and dignity of every child in our care
- Ensuring that children's images, names and personal information are never shared online without appropriate written consent
- Using social media as a positive tool for community engagement, communication and professional learning
- Setting clear and fair standards for staff conduct online
- Protecting the reputation and integrity of the service
- Complying with all relevant legislation, including the Privacy Act 1988 and child protection laws

---

SCOPE

This policy applies to:

- The approved provider, nominated supervisor, all educators, staff, contractors and volunteers
- Students on placement at the service
- All official service social media accounts and digital communications platforms
- Personal social media use by staff where it relates to the service, children, families or colleagues
- Any device used to access social media in connection with the service, whether service-owned or personal

Note: *'Social media' includes but is not limited to: Facebook, Instagram, TikTok, Snapchat, X (formerly Twitter), YouTube, LinkedIn, WhatsApp, WeChat, Messenger, private group chats, blogs, forums, parent apps and any other online platform where content can be posted or shared.*

LEGISLATIVE REQUIREMENTS

Education and Care Services National Law Act 2010

- Section 167: Protection from harm and hazards
- Section 174: Offence to fail to notify certain circumstances to the Regulatory Authority
- Section 273: Duty of confidentiality — staff must not disclose protected personal information

Education and Care Services National Regulations 2011

- Regulation 84: Awareness of child protection law
- Regulation 155: Interactions with children
- Regulation 168: Education and care service must have policies and procedures
- Regulation 170: Policies and procedures to be followed
- Regulation 171: Policies and procedures to be available

National Quality Standard

- Quality Area 2 — Children's Health and Safety: Element 2.2.1 — Children are protected from harm and hazard at all times
- Quality Area 4 — Staffing Arrangements: Element 4.2.2 — Educators, co-ordinators and staff members work collaboratively and demonstrate an understanding of the service's philosophy and practice
- Quality Area 6 — Collaborative Partnerships with Families and Communities: Element 6.1 — Respectful relationships with families are developed and maintained
- Quality Area 7 — Governance and Leadership: Element 7.1.2 — Management systems are in place to monitor compliance with legislation and policies

Privacy and Child Protection Legislation

- Privacy Act 1988 (Cth) — Australian Privacy Principles (APPs), including APP 3 (collection), APP 6 (use and disclosure) and APP 11 (security)
- Children and Young Persons (Care and Protection) Act 1998 (NSW)
- Child Protection (Working with Children) Act 2012 (NSW)
- Defamation Act 2005 (NSW) — online posts may constitute defamation
- Copyright Act 1968 (Cth) — use of images and content online
- Work Health and Safety Act 2011 (NSW) — online conduct that creates psychological harm may constitute a WHS breach

KEY DEFINITIONS

Term	Definition
Social Media	Any online platform or digital tool that allows users to create, share or interact with content, including text, photos, videos and links. This includes public platforms (Facebook, Instagram, TikTok), messaging apps (WhatsApp, Messenger) and any private online groups related to the service.
Official Service Account	Any social media account, page, group or profile created and operated in the name of the service, including accounts managed by staff on the service's behalf.
Personal Account	A social media account operated by a staff member in their own name or for personal use, not officially associated with the service.
Image / Video of a Child	Any photograph, video recording, screenshot, or other visual media that depicts or could identify a child enrolled at the service.
Written Consent	Express, informed permission provided in writing by a parent or guardian before a child's image, name or identifying information is used or shared. Consent must be specific about how, where and for what purpose the information will be used.
Identifying Information	Any information that could directly or indirectly identify a child or family, including: name, photo, suburb/address, school, siblings' names, disability or health information, family circumstances, or any combination of details that together could identify someone.

Cyberbullying	The use of digital technology to bully, harass, threaten, humiliate or target another person.

POLICY PROCEDURES

1. Children's Images, Videos & Privacy

⚠ **Important: This is the most critical section of this policy. The safety and privacy of children must always come first.**

1.1 Consent Requirement

Our service will never post, share or publish images, videos or identifying information about any child without prior written consent from the child's parent or guardian. This applies to:

- All official service social media accounts and websites
- All staff personal social media accounts
- Any online group, forum, app or messaging platform
- Any other digital or online medium

Written photo and media consent will be:

- Obtained during the enrolment process via a dedicated Photo and Media Consent Form
- Reviewed and updated annually or when the family's circumstances change
- Specific about the purposes for which images may be used (e.g. service website, Facebook page, newsletter, educational documentation) — blanket consent is insufficient
- Stored securely in the child's enrolment file
- Able to be withdrawn by the family at any time in writing

1.2 When Consent Has Been Given

Even where written consent has been provided, the following rules apply to all posts involving children:

- Never include a child's full name in the caption or tags of a photo
- Never include location information (suburb, street, school name) alongside a child's image
- Never post images that could compromise a child's dignity or be used to embarrass or harm them
- Avoid showing children in swimwear, undressed or in positions that could be misused
- Do not tag a child's location or check in at the service when children are present
- Review all photos carefully before posting — check backgrounds for other children who may not have consent
- Only post images where the primary educational or community purpose is clear

1.3 When Consent Has NOT Been Given

If a family has not provided consent, or has withdrawn consent:

- No images or videos of that child may be posted or shared under any circumstances
- The child must not appear — even incidentally — in the background of any posted image
- Staff must check enrolment records before posting any image involving a group of children
- If it is not possible to blur or exclude the child from a photo, that photo must not be posted

1.4 Special Circumstances

The following additional protections apply regardless of consent:

- Children who are on court orders (e.g. family violence orders, custody arrangements) may have strict restrictions on their image being shared — the approved provider must be consulted before any image of these children is used
- Children in out-of-home care (foster care) must never have their images shared publicly under any circumstances

- The service will never share a child's image alongside any information about their health, disability, family circumstances or behaviour

2. Official Service Social Media Accounts

2.1 Account Management

- All official service social media accounts must be approved and authorised by the approved provider
- Account login credentials (username and password) will be held by the approved provider and at least one other authorised person
- Two-factor authentication (2FA) must be enabled on all official accounts
- A register of authorised administrators will be maintained and reviewed annually
- When a staff member leaves, their access to all official accounts must be removed immediately
- Account passwords must be changed whenever an administrator leaves the service

2.2 Content Standards

Content posted on official service accounts must:

- Reflect the service's values, philosophy and professional standards
- Be approved by the nominated supervisor or approved provider before posting
- Be accurate, respectful and appropriate for a diverse community
- Promote the educational program and positive outcomes for children
- Celebrate children's learning without identifying individual children (unless consent obtained)
- Avoid controversial political, religious or divisive content that does not relate to early childhood education
- Never disclose confidential information about children, families or staff
- Comply with all copyright requirements — only use images and content the service has the right to use

2.3 Responding to Comments and Messages

- Only authorised staff may respond to comments or messages on official accounts
- Responses must be professional, respectful and timely
- Negative, offensive or inappropriate comments may be hidden or deleted — do not engage in arguments publicly
- Any comment or message that raises a child protection concern, complaint or safeguarding issue must be escalated to the nominated supervisor immediately — do not respond publicly
- Do not share personal or confidential information in response to public comments or messages
- If in doubt about how to respond, consult the nominated supervisor or approved provider before replying

2.4 Crisis and Emergency Situations

- During or following a serious incident or emergency, no information about the incident may be posted on social media without the express approval of the approved provider
- All media enquiries must be referred to the approved provider or designated spokesperson
- Photos, videos or details of incidents involving children must never be shared on social media
- The service's Emergency and Evacuation Policy takes precedence — social media must not be used in a way that interferes with emergency response

3. Staff Personal Social Media Use

Note: *This section applies to staff members' personal social media use where it intersects with their work at the service. Staff have the right to a private personal life online — this policy only addresses conduct that affects the service, children, families or colleagues.*

3.1 Absolute Prohibitions — Personal Accounts

The following are strictly prohibited at all times, including outside working hours:

	PROHIBITED CONDUCT
✕	Posting, sharing or tagging any image, video or information about a child enrolled at the service without written consent
✕	Identifying or naming any child enrolled at the service in any online post, comment or message
✕	Sharing any confidential information about children, families or colleagues obtained through your employment
✕	Making negative, derogatory, discriminatory or defamatory comments about children, families, colleagues, the service or competitors
✕	Sharing images taken inside the service premises (including learning environments, children's artwork displays, staff areas) without approval
✕	Engaging in cyberbullying, harassment or intimidation of any colleague, family member or community member
✕	Posting content that could bring the service into disrepute or undermine community trust in the service
✕	Connecting with families of enrolled children via personal social media accounts (e.g. accepting friend requests, following family accounts) without prior approval from the approved provider
✕	Sharing your personal views on matters relating to the service in a way that could be taken as representative of the service's position
✕	Using service Wi-Fi or devices to access personal social media during work hours except during authorised breaks

3.2 Expectations for Personal Conduct Online

Staff are expected to:

- Conduct themselves online with the same professionalism they bring to their role at the service
- Remember that online content can be permanent, widely shared, and may be seen by families, colleagues and the community
- Be mindful that their online presence as an early childhood educator reflects on the profession and the service
- Raise any concerns about colleagues' online conduct with the nominated supervisor, not address them publicly online
- Seek guidance from the nominated supervisor if unsure whether a personal post may breach this policy

3.3 Connecting with Families Online

Staff must not initiate or accept personal social media connections with families of enrolled children unless:

- The family member was known to the staff member personally before the child was enrolled at the service
- Written approval has been obtained from the approved provider

Where a personal connection with a family pre-exists enrolment, staff must:

- Declare the connection to the nominated supervisor

- Ensure that no information about the child's enrolment, development or behaviour is shared via personal social media
- Maintain professional boundaries in all online interactions

3.4 Professional Use of Social Media

The service encourages staff to use social media professionally for:

- Connecting with professional networks (e.g. LinkedIn, professional Facebook groups for early childhood educators)
- Accessing professional development resources, webinars and industry news
- Sharing publicly available resources relevant to the early childhood education sector

When engaging professionally online, staff should:

- Be clear that any views expressed are their own and not those of the service
- Not disclose any confidential service information
- Maintain the same respectful and professional standards they bring to their role

4. Photo and Media Consent Procedure

Step 1 — Obtain Written Consent at Enrolment

At enrolment, families will be provided with a Photo and Media Consent Form that specifies:

- What types of media may be captured (photos, videos, audio recordings)
- Where and how the media may be used (e.g. service Facebook page, website, newsletter, internal documentation, regulatory documentation, educational apps such as OWNA Storypark or SeeSaw)
- Who will have access to the media
- How long the media will be retained
- That consent can be withdrawn at any time in writing
- That consent does not extend to platforms or uses not listed on the form

Step 2 — Record and Store Consent

- Consent forms must be stored securely in each child's enrolment file
- A summary of consent status for each child must be accessible to all staff (e.g. on a consent register or in the service's management system)
- Staff must check consent status before taking or using any image of a child

Step 3 — Review Consent Annually

- Families will be asked to review and re-confirm consent during the annual enrolment review
- Any changes to how media is used (e.g. adding a new platform) must trigger a new consent process
- Families may withdraw consent at any time — withdrawal must be recorded immediately and all existing images of that child removed from public platforms as soon as practicable

Step 4 — Before Posting Any Image

Before publishing any image or video on a public platform, the staff member or nominated supervisor must:

- Confirm written consent is on file for every child appearing in the image (including children in the background)
- Ensure no child's full name, location or identifying information accompanies the image
- Review the image for anything that could compromise a child's dignity or safety
- Obtain approval from the nominated supervisor or approved provider

5. Reporting Concerns, Breaches and Complaints

5.1 What to Report

Staff must report the following to the nominated supervisor immediately:

- Any social media post (by staff, families or others) that includes a child's image, name or information without consent
- Any social media post that discloses confidential service information
- Any post or comment that may constitute cyberbullying, harassment or defamation
- Any social media activity that raises a child protection concern
- Any suspected breach of this policy by a staff member, student or volunteer
- Any online contact from a person of concern (e.g. someone attempting to access information about children)

5.2 Response Procedure

Upon receiving a report, the nominated supervisor or approved provider will:

- Assess the nature and severity of the concern
- Where possible, take immediate steps to have the content removed (contact the poster directly, report to the platform, or seek legal advice if necessary)
- If the content involves a child protection concern, notify the NSW Child Protection Helpline (132 111) and, if required, Police
- Document the incident including screenshots, dates and times as evidence
- Notify the affected family as soon as practicable
- Notify the Regulatory Authority (NSW Early Childhood Education Directorate) if the breach constitutes a serious incident under the National Law
- Review and update this policy if the breach reveals a gap in current practice
- Take appropriate disciplinary action in accordance with the service's disciplinary procedures if the breach was caused by a staff member

5.3 Disciplinary Consequences

Breaches of this policy by staff, volunteers or students may result in:

- A formal warning
- Requirement to complete additional training
- Removal of access to service social media accounts
- Referral to the Working With Children Check authority
- Termination of employment or placement
- Referral to police or child protection authorities in serious cases

⚠ Important: Sharing a child's image online without consent is not just a policy breach — it may be a breach of the Privacy Act 1988 and child protection legislation, and may result in serious legal consequences.

6. Families and Social Media

We ask families to be aware of and respect the following when using social media in relation to our service:

Expectation for Families	Applies?
Before posting any photo or video taken at the service (e.g. at a concert, excursion or event), check with other families present to ensure no other children appear without their family's consent	[ ] Yes [ ] No
Do not share images of other people's children on your personal social media without that family's consent, even if taken at a service event	[ ] Yes [ ] No
Do not post negative, defamatory or harmful comments about the service, educators or other families in any public online forum	[ ] Yes [ ] No

If you have concerns about the service, please raise them directly with the nominated supervisor or approved provider rather than via social media	[ ] Yes [ ] No
Do not share information about other children's behaviour, health or family circumstances in any online group	[ ] Yes [ ] No
Inform the service immediately if you see content online that you believe may harm a child at the service or breach their privacy	[ ] Yes [ ] No

Note: *The service may operate a private, closed parent communication group (e.g. via an approved app or closed Facebook group). Families who are invited to join this group agree to keep all content shared within it confidential and not to share it externally.*

EDUCATOR AND STAFF RESPONSIBILITIES

Approved Provider

Approve and oversee all official service social media accounts; hold master login credentials; approve significant content before posting; take final responsibility for policy compliance; manage serious breaches and regulatory notifications; review this policy at least every two years.

Nominated Supervisor/Person in Day to Day Charge

Manage day-to-day oversight of official accounts; approve content before posting; ensure all staff are trained in this policy; receive and act on breach reports; maintain the consent register; liaise with families regarding consent; escalate serious concerns to the approved provider.

All Educators and Staff:

Read, understand and comply with this policy; check consent records before taking or sharing any image; report any suspected breach or concern immediately; complete social media training during induction and annually; sign the Staff Social Media Acknowledgement Form.

Families:

Provide written consent for their child's image use; inform the service immediately of any concerns about online content; respect the privacy of other children and families when using social media in connection with the service.

RELATED POLICIES AND PROCEDURES

- Privacy and Confidentiality Policy
- Cybersecurity and Data Protection Policy
- Child Safe Environment Policy
- Staff Code of Conduct
- Interactions with Children Policy
- Dealing with Complaints Policy

- Record Keeping and Documentation Policy

REFERENCES AND RESOURCES

- ACECQA — Policy Guidelines: acecqa.gov.au
- Office of the Australian Information Commissioner (OAIC) — Privacy: oaic.gov.au
- eSafety Commissioner — Online safety for educators and services: esafety.gov.au
- NSW Office of the Children's Guardian — Child Safe Standards: ocg.nsw.gov.au
- NSW Child Protection Helpline: 132 111
- Australian Human Rights Commission — Photography and Privacy: humanrights.gov.au

POLICY REVIEW

This policy will be reviewed at least every two years, or more frequently following:

- A social media incident or breach involving the service
- Changes to legislation, regulations or best practice guidelines
- Feedback from staff, families or the regulatory authority
- Introduction of new social media platforms or communication tools used by the service
- Regulatory assessment and rating visit

Date policy was last reviewed: 19/02/2026
Date for next review: 19/02/2028
Reviewed by: Director and Staff