Social Media and Email

Every child is a precious trust

Background

Sunkids provides an internet email system to support its activities and access to this system is granted to company employees on this basis. Emails sent or received on Sunkids email system are not private property; they form part of the administrative records of Sunkids. Incidental and occasional use of the corporate email is subject to the restrictions contained in this policy.

The use of social media such as Facebook, MySpace, LinkedIn, YouTube, Twitter, Weblogs, Flickr and Instant Messaging (including SMS) has increased significantly in recent years.

Approved Providers generally accept that staff will use social media in their personal lives to keep in touch with friends, share ideas and engage in online discussions. However, they also recognise the potential for damage that misuse of social media can cause to their business, staff members, children, and families. Such damage can be occasioned when the comments are untoward, and the staff members can be identified with the Service.

All staff need to be aware that they are personally responsible for the content they publish in a personal capacity on any social media platform. They also need to accept that any comments they post are usually available to a far wider audience than intended.

Policy statement

This policy aims to ensure that the Service, children, staff, and families are protected from being compromised in any form of social media. It provides guidelines for the publication of, and commentary on, social media by staff and others who can be identified as being connected with the Service. To ensure that employees of Sunkids understand the way in which electronic mail (email) and the internet should be used in the organisation. It aims to ensure that email is used effectively for its intended purpose without infringing legal requirements or creating unnecessary business risk and that internet access is limited to work related matters only.

Strategies and practices

- All employees of Sunkids including contractors and temporary staff are subject to this policy. At the same time, your conduct and/or action(s) may be unlawful or illegal and you may be personally liable.

- Child Safety in the Digital Space, Employees must not share, post or store any digital content (text, images, videos, recordings) of children or their families on any platform—personal or professional—unless explicitly authorised in writing, in accordance with our Photographs and Video Recording Policy."

- Child-Safe Digital Practices –

  Restrictions on sharing images and identifiable details online.

  Risks of indirect identification even when names are omitted.

  Mandatory use of secure, approved platforms for digital sharing (e.g. OWNA)

- Sunkids provides an internet email system to support its activities and access to this system is granted to company employees on this basis. Emails sent or received on Sunkids email system are not private property; they form part of the administrative records of Sunkids. Incidental and occasional use of the corporate email is subject to the restrictions contained in this policy.

- Any personal use of email and the internet is not permitted. Use of the system must not detrimentally affect the job responsibilities of other employees, disrupt the system and/or harm Sunkids reputation.

- Care should be taken when using email because email messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Bear in mind that all expressions of fact, intention and opinion via email can be held against you and/or Sunkids in the same way as verbal and written expressions. Formal methods of email distribution must not be used for sending emails that are not relevant to the business. Access to all email internet sites (e.g., Hotmail, Yahoo mail etc.) is prohibited due to the potential threat of viruses being spread and infecting the network. Emails to families must also be treated as confidential.

- All information relating to educators, children, families, and the business operation of Sunkids is confidential. You are expected to treat electronic information with the same care as you would paper-based information which is confidential. Keep all such information secure, use it only for the purpose(s) intended and do not disclose the same to any unauthorised third party, which may sometimes include other employees of Sunkids.

- Keep passwords safe. Do not disclose them to anyone.

- If a document is highly confidential or sensitive in nature, you should store it in a private directory. Do not forward, send or in any way disseminate such information that may compromise Sunkids.

- Maintain confidentiality by not forwarding or sharing any client information that would violate the *Data Protection Act* or industry guidelines.

- Return any message received that was intended for another recipient. Delete any copies of misdirected messages. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

- Verify the recipients of the email are approved to receive the information contained in the email, to avoid a breach of confidence.

- Exercise due care when writing an email to avoid being rude or unnecessarily terse and ensure that your message meets the standards of professionalism Sunkids expects of your position.

- Do not make any statements on your own behalf or on behalf of Sunkids, which do or may defame label or damage the reputation of any person or the organisation.

- Do not engage in any activity that is illegal, distasteful, or likely to have negative repercussions for Sunkids.

- Email messages and internet traffic that has been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending material

can be identified. Emails, both in hard copy and electronic form, are admissible in a court of law.

Social Media Conduct Related to Child Safety

- **NQF Expectation**: Sunkids have strong boundaries and duty of care when representing the service in personal social media use.
- *When participating in social media, staff must not e*ngage in any digital conduct that could place a child at risk of emotional, psychological or physical harm.
  All online interactions with families must remain strictly professional and occur only via authorised communication channels such as work email and/or OWNA

Professional Boundaries and Digital Behaviour

- Staff must model respectful relationships and understand how digital conduct may affect children and families.
- In the "Harassment, Bullying and Discrimination" section, add:
-

GUIDELINES FOR USE

- Internet and email may be used by an educator for the conduct of the business, as detailed above.

- Used by educators in the preparation and enhancement of the Sunkids curriculum or the provision of care, e.g. children are interested in information about a topic and the educator uses the internet to find facts to include in the project, or educator uses email to contact an organisation who can provide information that will be used for the children's benefit.

- Usage must be in allocated programming time or in the educator's personal time

PROCEDURE FOR USE

1. Advise the Nominated Supervisor that you will be using the internet/email
2. Arrange to have access in program preparation time or personal time
3. Use the Service log to record usage and have Nominated Supervisor sign off

MONITORING

- All Sunkids resources, including computers, email and voicemail are provided solely for business purposes. At any time and without prior notice, Sunkids maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by Sunkids. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.

- In order to ensure compliance with this policy, Sunkids may employ monitoring software to check on the use and content of emails to ensure that there are no serious breaches of the policy. Sunkids specifically reserves the right for authorized personnel to access, retrieve, read and delete any communication that is created on, received through or sent through the system, to assure compliance with all company policies. Such monitoring will be used for legitimate purposes only.

Social Media and Email

Every child is a precious trust

GENERAL EMAIL MAINTENANCE

- Policy will include an email size limit for all users except for graphic works emails which contain images for Sunkids. (10 Mb Limit)
- Email users are requested to delete all items residing in the deleted items folder and to delete where applicable any emails in their sent items box.
- Email users can add the size column to any mailbox.
- By right clicking on the grey column area next to received, select field chooser, and then scroll down to find "size". Click and hold on the word "size" and drag to the area next to received. Let go of the mouse and the size column will be added. You can now sort your emails by size by single clicking on the size column. This will allow the user to determine which emails are oversize and should be deleted. Delete all emails larger than 1Mb if possible.

When participating in social media, staff should: -

- Be respectful to and about others at all times.
- Assume that the comments they post may be available to persons other than those for whom the communication was intended.
- Be certain not to disclose other people's personal information or publish images of others without permission.
- Recognise that a person may be readily identifiable even when not named.
- Re-read and re-consider what is being said before posting it.

When participating in social media, staff must not: -

- Imply they are authorised to speak for the Service nor for the Approved Provider.
- Use the Services email or any logos or branding pertaining to the Service when conducting personal business or expressing personal views.
- Use the identity or likeness of another employee, customer, supplier, or business partner, etc.
- Publish or report on conversations or information that is deemed confidential or classified or deals with matters that are internal in nature.
- Use or disclose any information, including photographs or videos, relating to children and families, other staff or anyone connected with the Service, obtained through your employment at the Service.
- Make any comment or post any material that might otherwise cause damage to the Approved Provider's reputation or bring the Service into disrepute. This includes any comments that are defamatory, harassing, bullying, discriminatory, insulting, obscene or in any other way harmful.

The following activities are expressly forbidden: -

- The introduction of any form of computer virus.
- Seeking to gain access to restricted areas of the network or other hacking activities.
- Forgery or attempts to read other users' mail without their expressed permission.
- Accessing websites and emails that are not for work related purposes or for the benefit of the Service. Such prohibited sites include, but are not limited to, Instagram, My Space, Facebook, Hotmail, YouTube and Yahoo.
- Creating any website pages that can be linked to Sunkids.
- Using confidential records from the Service such as photos or documentation that could make their way into the public domain.

- Contacting families by email or text message for any purpose other than requested information, as per the enrolment form, related to their child, account details or newsletters.
- Contacting families for personal or social reasons.

Identifying inappropriate use

- Staff who notice inappropriate or unlawful content online in any way relating to the Service, or content that may be in breach of this policy, should inform the Nominated Supervisor immediately.

Harassment, bullying and discrimination

- Abusive, harassing, threatening, or defaming postings which are in breach of any of the Services policies may result in disciplinary action being taken, even if such comments are made using private social networks outside of working hours. All staff and others connected with the Service are expected to treat each other with respect and dignity and ensure their behaviour both online and while at the Service does not constitute unlawful discrimination, bullying or harassment in any form.

  Staff must refrain from liking, commenting on, or interacting with families' social media content where such engagement could compromise professional boundaries.

Access to social media at the Service

- The services computers and other communication devices are for work purposes only, and not for conducting personal business or for participating on social media websites during working hours or otherwise.
- Staff are not to use their personal mobiles, computers, or other electronic devices to access social media in any form during rostered work hours.
- Staff are not to use personal cameras, mobile phones, or other electronic devices to take photographs while at the Service or on excursions. Refer to the Services Photographs and Video Recording Policy.
- There are no restrictions in place on educator's ability to wear smart watches as their choice of timekeeper while in the workplace, however that should be their sole use during work hours. Educators are asked to consider the use of their smart watches in line with the use of their personal mobile phones during work hours. Smart watches must have all notifications turned off during work hours, if this is not possible their use must be limited to that of a time keeping device only. If an educator is unable to fulfill these restrictions, they may be asked to remove their smart watch whilst on duty.
- The use of headphones of any form, including wireless earpieces, is not permitted during an educator's work hours. These devices limit educator's ability to appropriately supervise children's interactions.
- Any personal device use that distracts from or reduces vigilance in supervision is a breach of duty of care.

Digital Child Safety and Risk Management

As part of our commitment to maintaining a child-safe organisation, Sunkids applies rigorous controls around digital communications, access, and representations involving children. All staff must uphold child-safe principles when using digital technologies and report any breaches or concerns involving the digital safety of children.

Mandatory Reporting of Digital Risk

If any staff member becomes aware of online content (on any platform) that may indicate a child is at risk of harm—whether through grooming, exposure to inappropriate material, or digital bullying—this must be reported immediately to the Nominated Supervisor and in accordance with our Child Protection Policy.

Breach of Policy

- Any staff member whose actions are deemed to be in breach of this policy could face disciplinary action.
- Where necessary, disciplinary action will be determined by the Approved Provider according to the circumstances of the case. Counselling, mediation, training, re-training and the issue of written warnings may be considered by the Approved Provider as possible remedies. In severe circumstances, failure to act in accordance with this policy could result in termination of employment.

Additional safe practices for babies

- N/A

Responsibilities of parents

- To act in accordance with this policy.
- To report any inappropriate or unlawful content online relating to the Approved Provider or the Service, or content that may be in breach of this policy, to the Nominated Supervisor.

Procedures and forms

- Internet/Email Usage Log
- Agreement to the Social Media and Email Policy

Links to other policies

- Child Protection and Risk Management Policy
- Educator Professionalism and Ethics Policy
- Enrolment and Orientation Policy
- Photographs and Video Recording Policy
- Privacy and Confidentiality Policy
- Students, Volunteers and Visitors Policy
- Child-Safe Environments Policy
- Cyber Safety Policy
- Use of Electrical and Other Equipment Considering Child Safe Risks
- Photographs and Video Recording Policy

Links Education and Care Services National Regulations 2011, National Quality Standard 2018

Regs	181	Confidentiality of records kept by approved provider
	183	Storage of records and other documents

QA	2.2.3	Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect
	4.2.1	Management, educators and staff work with mutual respect and collaboratively, and challenge and learn from each other, recognising each other's strengths and skills
	4.2.2	Professional standards guide practice, interactions and relationships
	5.1.2	The dignity and rights of every child are maintained
	7.1.2	Systems are in place to manage risk and enable the effective management and operation of a quality service
	7.2.3	Educators, co-ordinators and staff members' performance is regularly evaluated, and individual plans are in place to support learning and development

Sources

- Education and Care Services National Regulations 2011
- Guide to the National Quality Standard 2018
- Revised NQF Policy Framework 2025

Further reading and useful websites

- Office of the Australian Information Commissioner. *Read the Australian Privacy Principles* https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles/ assessed 9 July 2024

Policy review

The Service encourages staff and parents to be actively involved in the annual review of each of its policies and procedures. In addition, the Service will accommodate any new legislative changes as they occur, and any issues identified as part the Service's commitment to quality improvement. The Service consults with relevant recognised authorities as part of the annual review to ensure the policy contents are consistent with current research and contemporary views on best practice.

Version Control

Version	Date Reviewed	Approved By	Comments/Amendments	Next Review Date
1	8 January 2018	Kaylene Harper	Updated to changed NQF requirements 1 February 2018. Service to modify policies to its specific needs.	January 2019
2	6 February 2019	Kaylene Harper	Policy reviewed. Sources and further readings accessed and updated.	February 2020
3	31 January 2020	Kaylene Harper	Policy reviewed. Sources and further readings accessed and updated.	January 2021
4	14 October 2020	Kaylene Harper	Policy reviewed. Sources and further readings accessed.	October 2021
5	17 June 2021	Kaylene Harper	Additional information regarding smart watches and headphones added.	June 2022
6	22 September 2021	Kaylene Harper	Policy reviewed	September 2022
7	30 September 2022	Linda Hollard	Policy reviewed	September 2023
8	23 August 2023	Grace McKinstray	Policy Reviewed. Further readings accessed.	August 2024
9	9 July 2024	Tiffany Boeske	Reviewed policy Accessed sources	July 2025
10	20 June 2025	Kaylene Harper	Revisions aligned to 2025 NQF Child Safe Policy changes, including enhanced digital child safety and staff responsibilities	June 2026