BEFORE, AFTER & VACATION CARE

MULTIMEDIA USE AND STORAGE POLICY

TEAMKIDS | AUG 2025

FUN GENUINE INNOVATIVE INVOLVED REMARKABLE

MULTIMEDIA USE AND STORAGE POLICY

POLICY RATIONALE

At Team Holiday Pty Ltd and its associated entities, including TeamKids, Kids Unlimited and Stand Up Project ("the Company") recognises that child safety is the responsibility of everyone, including the Company, and all Managers, Educators, and Volunteers who come into contact with children or child related information. This policy ensures that clear standards are adhered to when it comes to the safety, wellbeing, and privacy of all children in attendance at Company operated services.

This policy will outline how the Company will obtain and manage consent to take or record images of children, including the supervision of children during the times in which images or recordings are being taken. These expectations will be in line with the National Model Code, Principle 8 of the National Principles for Child Safe Organisations, and all state Child Safe Standards to ensure best practice in accordance with the facilitation of a child safe environment.

In addition to the above codes, principles and standards, this policy will be used in partnership with the Risk Assessment – National Model Code – Use of electronic equipment and storage of images/videos of children. This Risk Assessment will include the appropriate use of service issued electronic devices, creation of a child safe culture, and the use of personal electronic devices when working or volunteering with the Company.

The Company acknowledges that while images of children may be taken for genuine reasons such as program development, documentation of child engagement within a program, and for approved marketing purposes, there may be risk of images or recordings of children being used inappropriately. This policy ensures that children are protected from having those images used inappropriately, in particular, that they are protected from the taking or sharing of inappropriate or illegal images.

TeamKids recognises that media and technology in all its forms can provide both entertainment and education to children, provided that the material viewed or heard is age appropriate and supervised.

THE COMPANY WILL:

- Ensure each TeamKids service is issued with a TeamKids registered mobile phone, tablet and laptop which are monitored, secured and maintained by TeamKids' internal IT team. Apps cannot be added to these devices, except through TeamKids Head Office action.
- Provide maintenance on equipment, as well as phone and email support to team members to assist them in the use and upkeep of this equipment. Children are not to access the service electronic devices unless under direct supervision of an educator at all times when they use the electronic device.
- Ensure that management conducts regular checks at each service to monitor personal phone use and confirm that all educators are complying with the requirements of this policy. This includes checking that all educators have stored their personal devices securely in the designated location and personal devices are not being used for images, videos and recordings.
- Encourage all educators to report any misuse of personal devices to management immediately.
- In conjunction with the school in which the service is located, ensure that the use of optical surveillance devices such as CCTV is only permitted for safety, security, and supervision. Ensure that CCTV systems in place at a service are compliant with applicable privacy laws, not located in private areas (e.g., bathrooms), and footage access is restricted to authorised personnel.

- Investigate reports related to alleged breaches of this policy or misuse of personal or TeamKids issued electronic devices.

Destruction of images, videos, and recordings:

When images, videos or recordings are no longer required for the purpose they were collected, TeamKids follows Australian Privacy Principles and the National Model Code by securely destroying such materials from the secure platform it is stored.

TeamKids uses secure internally monitored and controlled systems, on all TeamKids registered devices to ensure images, videos and recordings of children can be stored and destroyed appropriately.

We further confirm that:

- Images taken on TeamKids registered devices including phones and tablets are stored on the device internally, not memory cards, and can only be stored on our internally managed OneDrive system. Images are deleted directly from the device and permanently destroyed. Once images they have been used for their intended purpose, they are then permanently destroyed.
- Images stored on TeamKids registered laptops are stored internally and securely via our internally controlled OneDrive system. Images are deleted from these locations once they have been used for their intended purpose, and are then permanently destroyed.
- Images taken for the purpose of incident/injury reports/ Police or Child protection agencies will be kept securely on internally managed TeamKids OneDrive until the child turns **25 years of age.** Images will then be deleted from the secure TeamKids managed OneDrive system to ensure they are permanently destroyed.
- Images taken for the purpose of marketing are stored internally and securely via our internally controlled OneDrive system. Images will be kept securely until no longer required, before they are deleted from the secure TeamKids Onedrive system to ensure they are permanently destroyed.
- Where images are being taken for the purpose of Media or marketing, parental consent will be gained via agreement on the child's enrolment record. Families will be notified if an outside agency seeks consent to collect images, audio and or video.
- Organisations engaged by TeamKids for the purpose of marketing, will be provided with an agreement to abide by the terms of this policy.
- The Company will ensure personal devices are not approved for use as official service devices.

SERVICES WILL:

- Ensure that any media viewed within the service or during excursions is rated G or PG, with parent/guardian approval obtained. For G-rated media, permission is provided within the enrolment terms and conditions.
- Only use visual median as part of a planned learning experience, supported by educators and followed up with related activities.
- Allow children to enjoy music within the service, while prohibiting music that contains derogatory content, inappropriate language, or sexual references.
- Use the TeamKids Spotify account to play music, ensuring all music is pre-approved by the person in day-to-day charge and/or Management to confirm suitability for primary school-aged children.
- Permit children to access the internet only with approval from the person in day-to-day charge and/or Management, in consultation with children, families, and/or management. At all times, educators must be

able to view children's screens and internet access should be limited to activities such as homework club or educational experiences.

- Allow children to use school-provided laptops or iPads for homework during set times and for set intervals. Educators must supervise, assess and monitor programs used to ensure age appropriateness.
- Ensure that children who require electronic devices for medical (e.g., phone, tablet, monitor) have access to them at all times under supervision.
- Use only TeamKids issued electronic devices to capture images, videos or recordings of children. This includes mobile phones, digital cameras, tablets, iPads, or other emerging technologies.
- Maintain TeamKids issued devices (e.g., mobile phones, iPads, memory storage devices) in the possession of TeamKids employees at all times. Any exceptions (e.g., for marketing purposes) must be essential, authorised in writing, and must not impede active supervision of children.
- Require the service Responsible Person to monitor the use of electronic recording devices and report any inappropriate use or policy breaches to the Regional Manager.

Use of images, videos and sound recordings

Children's images may be used to document children's learning including observations, reflection journals, and Quality Improvement Plans (QIP) in the course of providing its educational programs.

The Company may take photographs, videos and/or sound recordings of children.

This may include for the following purposes:

1) Records of child's participation
2) Reporting to parents and guardians
3) Documenting learning experiences
4) Sharing experiences within the TeamKids program through various media (e.g. newsletters, visual displays, emails).
5) Development of Company professional educational material for training purposes and internal TeamKids communications

These photographs, videos and sound recordings are not used by the Company for biometric matching or identification and are not provided to any third party. Photo consent for a child may be withdrawn at any time through the child's account.

EDUCATORS WILL:

- Keep passwords and security codes for phones, tablets, and laptops confidential and avoid sharing them with anyone outside of Company employees (e.g., not with children).
- Log out of laptops after each use to maintain digital security.
- Observe the photo permissions of each individual child's account, and adhere to these permissions at all times.
- Ensure that children remain supervised while taking images, videos, or recordings. Educators must ensure that children remain supervised and should avoid allowing these tasks to interfere with active supervision responsibilities.

- Under no circumstances use personal electronic devices to photograph, record or film children, including for the purpose of documenting learning.
- Never capture inappropriate images or videos of children, including in off-limits areas as defined in the service risk assessment. This includes avoiding situations where a child is:
    - Not fully or appropriately dressed (i.e. in their underwear, in a state of undress, completely undressed or with their genitalia exposed).
    - Positioned in a way that may be perceived as sexualised.
    - Experiencing visible distress, anxiety, or dysregulation.
- Adhere to the service risk assessment to avoid taking images or recordings in restricted areas such as bathrooms or nappy changing areas.
- Limit the sharing of child images or videos to platforms and purposes aligned with the original educational intent.
- Never transfer content to personal accounts or devices, including uploading to social media or other unauthorised platforms.
- Read and acknowledge this policy on their employment platform as part of their compliance responsibilities.
- Store personal mobile phones, digital cameras, tablets, wearables (camera glasses), smart watches with camera/recording functionality, SD cards, USB and hard drives securely in the service office space during operational hours, unless explicitly permitted by Company management under the approved conditions below.
- Use personal electronic devices only with prior Company authorisation, and only for the following approved purposes:
    - Communicating during an emergency (e.g. unaccounted child, serious injury, evacuation).
    - Managing personal health needs (e.g. heart or blood sugar monitoring).
    - Supporting disability-related needs (e.g. communication aids).
    - Responding to family emergencies (e.g. ill or dying family member).
    - Responding to a technology failure.
    - Receiving critical information during a local emergency (e.g. bushfire warnings).
- Follow protocols related to the storage and retention of images and videos of children, including:
    - Accessing only approved devices and platforms to view, move, or store files.
    - Using images and videos only for their intended educational or promotional purpose, and with appropriate consent.
    - Avoiding posting or sharing images or content through unauthorised platforms or applications.
    - Using only service-issued electronic devices for capturing and storing content.
    - Monitoring device use to ensure compliance with policies and reporting any breaches.

Educators and other staff can access personal electronic devices while taking a scheduled break from work, such as a lunch break, or during planning time, when they are not providing education and care or working directly with children.

Personal social media accounts

The Company does not recommend adding family members from the service as a ‘friend’ on Facebook or other social media platforms, however employees should use their discretion, noting that as Company employees, they may still be viewed as representatives of the Company outside of work hours, and are expected to uphold the Code of Conduct in all online interactions.

Under no circumstances is it appropriate for a Company employee to exchange contact information with a child, or to connect with a child on any form of social media or electronic communication. Any attempts made by a child to connect with or exchange contact details with a Company employee should be reported to the Manager, and child's Parent or Guardian immediately.

It is extremely important not to post information about the Service, colleagues, children, or families on personal social media accounts, as this not only contravenes the service policies and Code of Conduct but is considered a breach of the Commonwealth's Privacy Act 1988 and Privacy and Personal Information Protection Act 1998.

FAMILIES WILL:

- Refrain from taking photos or videos of children in the care of the Company unless prior written approval has been granted by the relevant parent or guardian for specific purposes such as marketing, developmental documentation, or special events. Any approved use must also comply with the policy's section on the destruction of images and videos.
- Observe signage displayed at the service entrance that advises all visitors, students, guardians, and external providers of the photography restrictions in place.
- Provide written permission if photos or videos of their child are required to be taken or shared with external professionals or agencies (e.g. NDIS, occupational therapists, inclusion support professionals). This written consent will be securely stored and displayed on the service communication board.
- Complete the image and video consent section of the child's enrolment record, which outlines how TeamKids will use and protect any media involving their child, in line with privacy and safety obligations.
- Ensure children's personal electronic devices (including smartwatches, phones, tablets, laptops, and cameras) are either not brought to TeamKids or stored in children's bags during their attendance at TeamKids. Parents can contact their child via the service mobile phone.

BREACHES OF POLICY

Any breach of this policy may result in disciplinary action, up to and including termination of employment.

This includes, but is not limited to, the inappropriate use, storage, sharing or destruction of images or recordings; failure to adhere to supervision requirements; and unauthorised use of personal or service devices.

All staff are expected to uphold the standards outlined in this policy at all times, and to act in accordance with the Code of Conduct, relevant legislation, and privacy regulations.

Suspected or confirmed breaches must be reported immediately to the appropriate Company Manager, People and Culture team or childsafety@teamkids.com.au.

Failure to comply with this policy may also result in legal action where breaches involve violations of child safety laws or privacy legislation.

REFERENCES

ACECQA National Quality Framework Resource Kit (2012)
ACECQA National Quality Framework – National Model Code (July 2024)
Quality Area 1 – Educational Program and Practice.
Quality Area 2 – Children's health and safety
Quality Area 7 – Leadership and Service Management
Victorian Child Safe Standards
Education and Care Services National Law Act (2010), S 165

Version control Date: August 2018

Reviewed: July 2025

To be reviewed: July 2026