POLICIES IN THIS SECTION AS REQUIRED BY:
Education and Care Services National Law (WA): 'Law': Section S.162A; S.165; S.167; S.175B; S.175C; S.175E and S.175F.

Education and Care Services National Regulations– 'Regulations':73;84;168(2)(ha);170-172;175-176;181;183-184.

National Quality Framework for Early Childhood Education and Care and School Age Care: Quality Area 1; Elements 2.2.1; 2.2.3; Element 7.1.2

Nature Alliance Family Day Care is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and the community. As a Child Safe Organisation, our Service embeds the National Principles for Child Safe Organisations and continuously addresses risks to ensure children are safe in physical and online environments.

Digital technologies have become an integral part of many children's daily lives. For this reason, it is important that our Educators and staff are not only familiar with the use of digital technologies, but are able to guide children's understanding of, and ability to interact, engage, access and use a range of digital technology in a child safe environment.

POLICY
Children's safety and wellbeing is paramount, and Nature Alliance Family Day Care has the responsibility to work with Educators and staff to provide and maintain a safe and secure working and learning environment for staff, children, visitors and contractors, including online environments. We aim to create and maintain a positive digital safe culture that works in conjunction with our Service philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, Educators and families.

Educators may choose to have Closed-Circuit Television (CCTV) installed at their registered premises/venue to address crime prevention strategies, to reduce concerns, to deal with complaints and support investigations.

Nature Alliance Family Day Care is committed to protecting personal information and will comply with the Privacy Act 1988 (Cth), Australian Privacy Principles and other applicable privacy requirements, to the extent they apply to the Service.

SCOPE
This policy applies to children, families, staff, Educators, Educator Assistants, the Approved Provider, students, volunteers and visitors to the Family Day Care Service.

DEFINITIONS
Appropriate steps and measures refers to actions that are reasonable and proportionate to the circumstances and the level of risk involved, intended to protect children's safety and privacy, secure digital devices and information, prevent unauthorised access or disclosure, and respond effectively to actual or suspected digital safety incidents. These actions may include restricting access, securing devices and records, preserving relevant evidence, reporting concerns and taking corrective action.

PROCEDURES

The Approved Provider and Service Management will:

- Ensure that the use of digital technologies and online environments within the Service complies with the Education and Care Services National Law, National Regulations, National Quality Framework and relevant child safety requirements.
- Support Family Day Care Educators to use digital technologies, including photography and video recording, for legitimate education and care purposes, provided relevant legislative requirements, parental authorisations and appropriate safeguards are met.
- Establish processes for the approval and use of Service-issued devices for staff and Service-authorised devices for Family Day Care Educators, including ensuring devices are configured in accordance with the Service's child safety and device security requirements, and maintaining appropriate records of authorised devices and their users.
- Establish and maintain processes for obtaining, recording and making parental/guardian authorisations relating to images and videos of children accessible to Educators, including any limitations or withdrawal of consent, and provide guidance to Educators regarding their responsibilities for checking and complying with these authorisations.
- Review CCTV and other optical surveillance arrangements disclosed by Educators, including their purpose, location, access arrangements and security measures, and require any identified risks to children's safety or privacy to be addressed before authorising their use.
- Identify, assess and manage risks associated with digital technologies and online environments, provide appropriate guidance and support to Educators and staff, and monitor and review relevant practices to support ongoing compliance and continuous improvement.
- Ensure that digital information and records, including images and videos of children, are managed in accordance with the Service's confidentiality, privacy, recordkeeping and data security policies.
- Establish processes for responding to, documenting and reporting digital safety concerns, incidents and breaches in accordance with applicable legislative requirements and relevant Service policies.

Family Day Care Educators will:

- Comply with this policy and all applicable legislative requirements relating to digital technologies, online environments, child safety, privacy and the taking and use of images and videos of children.
- Use digital technologies in a manner that supports children’s safety, wellbeing, learning and development, while maintaining appropriate supervision and professional boundaries.
- Only use digital devices authorised by Nature Alliance Family Day Care to take, store or transmit images and videos of children, and ensure these devices are used exclusively for education and care purposes, in accordance with applicable legislative requirements.
- Ensure that appropriate parental authorisations have been obtained before taking, using, storing or sharing images and videos of children, and comply with any conditions or limitations associated with those authorisations.
- Identify and manage risk associated with the use of digital technologies, including photography, video recording, online platforms and connected devices, and implement safeguards appropriate to the circumstances of their Family Day Care Service.
- Take reasonable precautions to prevent unauthorised access to, use, disclosure, loss or misuse of digital information, including images and videos of children.
- Use Service-approved systems and arrangements for storing, accessing and sharing children’s information and educational documentation, and ensure records are retained or disposed of in accordance with applicable requirements.
- Report any actual or suspected digital safety incident, privacy breach, unauthorised access, loss of information or inappropriate taking, use or disclosure of children’s images, videos or personal

information to Nature Alliance Family Day Care as soon as practicable, but no later than 24 hours after becoming aware of the incident, including incidents occurring outside normal office hours.

- Participate in relevant training, guidance and review processes, and cooperate with Service Management to maintain safe digital practices.
- Notify Nature Alliance Family Day Care of any changes to Service-authorised digital devices, including the replacement, loss, disposal or discontinuation of a device, or changes to its authorised use or access arrangements. Any new or replacement device must be authorised by the Service before being used to take, store or transmit images or videos of children.

1. SAFE USE OF DIGITAL DEVICES AND ONLINE ENVIRONMENTS

Nature Alliance Family Day Care recognises that digital technologies support the delivery of education and care, children's learning and development, communication with families and the administration of Family Day Care Services.

The Service supports the appropriate use of digital technologies, provided their use complies with legislative requirements and risks to children's safety, wellbeing, privacy and dignity are appropriately managed.

Authorisation and Use of Digital Devices

- Before authorising a digital device, Nature Alliance Family Day Care will obtain information about the device's intended use, access arrangements and security configuration, and assess whether the arrangements meet the Service's child safety and device security requirements. Authorisation will be documented and may be subject to conditions, review or withdrawal.
- A device must not be used to capture, store or transmit images or videos of children until its use has been authorised by Nature Alliance Family Day Care. The Service will maintain written records of device authorisations and any subsequent changes or withdrawals in accordance with applicable legislative requirements.
- Digital devices used to take, store or transmit images or videos of children must be either issued by Nature Alliance Family Day Care to staff members or authorised by the Service for use by Family Day Care Educators. These devices must be used exclusively for education and care purposes, in accordance with applicable legislative requirements.
- Nature Alliance Family Day Care will maintain a register of Service-issued and Service-authorised digital devices, including sufficient information to identify each device, its authorised user and any conditions associated with its use.
- Educators may use service-authorised digital devices to support educational documentation, children's learning experiences, communication with families and other legitimate education and care activities.
- Educators must not use personal digital devices to take, store or transmit images or videos of children while providing education and care.
- Personal digital devices may otherwise be used or kept within the Family Day Care environment only to the extent permitted by applicable legislation and Service requirements. Their use must not compromise children's safety, supervision or privacy.
- The use of digital technologies must not interfere with Educators' responsibilities to adequately supervise children and maintain a safe environment.
- When a Service-authorised digital device is no longer required for education and care purposes, Educators must notify Nature Alliance Family Day Care and ensure that any images, videos or other information relating to children and families are securely removed before the device is used for personal purposes, transferred to another person, sold or disposed of. This may involve restoring the device to factory settings, securely erasing stored information or destroying storage media where appropriate. Any records subject to legislative

retention requirements must be securely retained in accordance with the Service's Record Keeping and Retention Policy before information is removed from the device.

Online Environments and Digital Resources

- Educators will ensure that digital content, applications, websites and online resources used with children are appropriate to their age, developmental abilities, individual needs and the intended educational purpose.
- Reasonable precautions must be taken to protect children from inappropriate content, unsafe online interactions, unauthorised communication and other foreseeable risks associated with digital technologies.
- Educators must consider the privacy and security implications of digital applications, platforms and connected devices before using them in connection with children's education and care.
- Communication and sharing of children's information through digital platforms must occur in accordance with relevant Service policies, including the Social Media Policy, Data Security Policy and confidentiality and privacy requirements.
- Any concerns regarding the suitability, security or use of digital devices, applications or online environments must be brought to the attention of Service Management.

2. DIGITAL DEVICES USED BY HOUSEHOLD MEMBERS AND OTHER PERSONS

Nature Alliance Family Day Care recognises that Family Day Care operates within residential environments where household members, visitors and other persons may possess and use personal digital devices. Educators must take reasonable steps to protect children's safety, privacy and confidentiality when these devices are present or used within the Family Day Care environment.

- Educators must inform household members, visitors, students, volunteers and Educator Assistants of the Service's requirements regarding digital devices, children's privacy and the taking and sharing of images and videos.
- Household members and visitors must not photograph, film, record or share images or videos of children attending the Service without appropriate authorisation.
- Educators must take reasonable steps to prevent household members and other unauthorised persons from accessing children's images, videos, records or confidential information, including through shared devices, applications or connected technologies.
- Students, volunteers and Educator Assistants must not use personal or unauthorised devices to take, store or transmit images or videos of children while participating in education and care activities.
- Any use of Service-authorised devices by Educator Assistants, students or volunteers must be approved by Nature Alliance Family Day Care and comply with applicable legislative requirements and Service policies.
- Educators must consider the potential risks associated with digital devices used by household members and other persons, particularly where devices are capable of photographing, recording or transmitting images of children.
- Any concerns or suspected breaches involving digital devices belonging to household members or other persons must be reported to Service Management as soon as practicable, but no later than 24 hours after becoming aware of the incident, including incidents occurring outside normal office hours.

3. TAKING, USING, STORING AND DESTROYING IMAGES AND VIDEOS OF CHILDREN

Nature Alliance Family Day Care recognises that photographs and videos provide valuable opportunities to document children's learning, development, achievements and experiences, support educational programming and strengthen communication with families.

The Service supports Educators in taking and using images and videos of children for legitimate education and care purposes, provided appropriate authorisations, safeguards and risk management strategies are in place.

Taking Images and Videos

- Images and videos of children may be taken for legitimate education and care purposes, including educational documentation, observations, learning portfolios, communication with families and other activities authorised by the Service.
- Images and videos of children must only be taken using digital devices issued by Nature Alliance Family Day Care to staff members or authorised by the Service for use by Family Day Care Educators, in accordance with applicable legislative requirements and this policy.
- Before taking images or videos of children, Educators must check the relevant parental/guardian authorisations available through the Service's enrolment records or other approved authorisation processes. Educators must comply with any conditions, limitations or withdrawal of consent and seek clarification from Service Management where an authorisation is unclear or does not cover the intended purpose.
- Educators must consider the safety, privacy, dignity and wellbeing of children when taking images or videos, including the nature of the activity, the circumstances in which images are taken and the potential for inappropriate use or disclosure.
- Children's views, preferences and developing capacity to provide or withhold assent should be respected, having regard to their age and understanding.
- Educators must ensure that taking images or videos does not interfere with their responsibility to adequately supervise children.

Using and Sharing Images and Videos

- Images and videos of children may only be used or shared for purposes consistent with the authorisation provided by their parent or guardian and the Service's policies and procedures.
- Images and videos must not be published, distributed or disclosed to unauthorised persons.
- Any use of children's images or videos for promotional purposes, including websites, social media or other publications, must comply with the Service's Social Media Policy and relevant parental authorisations.
- Educators must take reasonable precautions to prevent the identification or disclosure of personal information about children and families beyond what has been authorised.

Storing and Destroying Images and Videos

- Images and videos of children must be stored securely, using arrangements consistent with applicable privacy, confidentiality, recordkeeping and data security requirements.
- Access to images and videos must be limited to persons authorised to access them for legitimate education and care purposes.
- Images and videos must not be retained, copied, transferred or stored for personal use or outside authorised arrangements.
- Images and videos of children will be retained for as long as reasonably necessary for their authorised purpose, unless they form part of a record required to be retained under applicable legislation.
- Where images or videos form part of a record subject to legislative retention requirements, they must be retained for the prescribed period in accordance with the Service's relevant recordkeeping policies.

- Images and videos that are no longer required for their authorised purpose, and are not subject to legislative retention requirements, must be securely deleted from Service-authorised devices and any other locations where copies are stored. Printed images must be securely destroyed. Where there is uncertainty regarding the retention or disposal of images or videos, Educators must seek guidance from Service Management before deleting or destroying them, in accordance with the Service's Record Keeping and Retention Policy.
- Where parental authorisation is withdrawn or amended, the Service and Educator will review the continued use, sharing and retention of relevant images and videos, having regard to the revised authorisation and any applicable legal obligations.

4. PARENTAL / GUARDIAN AUTHORISATIONS

Nature Alliance Family Day Care recognises the importance of respecting the rights and preferences of children and families regarding the taking, use, storage and sharing of images and videos of children.

The Service will ensure that appropriate parental authorisations are obtained and managed in accordance with legislative requirements and the individual circumstances of each child. Written authorisation must be obtained from a parent or other person authorised to provide consent before images or videos of a child are taken, used or stored for education and care purposes.

- Authorisations may be obtained through the Service's enrolment documentation or other approved processes and must clearly identify the purposes for which images or videos may be taken, used, stored or shared.
- Separate or additional authorisation will be obtained where the proposed use of an image or video falls outside the scope of an existing authorisation, including where required for promotional, public or other purposes.
- Parents and guardians will be provided with sufficient information to make an informed decision about the taking, use, storage and sharing of their child's images and videos.
- The Service will maintain appropriate records of parental authorisations, including any conditions, limitations, amendments or withdrawals of consent.
- Educators must be aware of and comply with the authorisations applicable to each child in their care.
- Parents and guardians may request changes to, or withdrawal of, an authorisation. Such requests will be managed in accordance with applicable legislative requirements and any relevant recordkeeping obligations.
- Where authorisation has not been provided, or has been withdrawn, images or videos of the child must not be taken or used for purposes requiring that authorisation.
- Educators will take reasonable precautions to ensure that children whose parents have not provided the relevant authorisation are not identifiable in images or videos taken or shared for those purposes.
- The Service will consider any additional privacy, cultural, legal or safety requirements affecting the taking or use of a child's images or videos, including relevant court orders or restrictions.
- Any uncertainty regarding an authorisation or its application must be discussed with the parent or guardian or referred to Service Management before the relevant image or video is taken, used or shared.

5. OPTICAL SURVEILLANCE DEVICES (INCLUDING CCTV)

Nature Alliance Family Day Care recognises that optical surveillance devices, including closed-circuit Television (CCTV), security cameras and video monitoring systems, may be used within Family Day Care environments for legitimate purposes, including security, safety and the protection of persons and property.

The Service supports the appropriate use of these devices, provided their operation complies with relevant legislation and appropriate safeguards are implemented to protect children's safety, privacy and dignity.

- CCTV and other optical surveillance devices that may capture images or videos of children must be disclosed to Nature Alliance Family Day Care and must not be operated for this purpose without prior authorisation from the Approved Provider. Any authorisation will take into account the location and purpose of the devices, access arrangements and identified risks to children's safety and privacy.
- Educators must advise Nature Alliance Family Day Care of any optical surveillance devices installed or proposed for use within their Family Day Care residence or approved venue, including devices that may capture images or videos of children. Devices that may capture children being educated and cared for must be authorised by the Approved Provider before being used for this purpose.
- The use of optical surveillance devices must be considered as part of the Service's assessment of the Family Day Care environment, with relevant risks identified and appropriate safeguards implemented.
- Educators must ensure that the location, operation and purpose of surveillance devices are appropriate, having regard to children's safety, privacy, dignity and the nature of the Family Day Care environment.
- Parents and guardians must be informed of the use of surveillance devices that may capture images or videos of children, including their general purpose and the areas being monitored. Appropriate signage or other notification arrangements must also be in place to inform persons entering the premises that surveillance devices are operating.
- Surveillance devices must not be installed or operated in areas where children or other persons have a reasonable expectation of privacy, including bathrooms, toilets and areas used for changing or personal care.
- Where surveillance devices capture images or videos of children, the recording, access, use, storage, disclosure and destruction of that material must comply with applicable legislative requirements and the Service's relevant policies and procedures.
- Access to surveillance footage must be restricted to persons with a legitimate and authorised reason to access it.
- Surveillance footage must not be used, copied, shared or disclosed for purposes unrelated to its authorised use, except where required or permitted by law.
- Surveillance footage may be accessed or disclosed where reasonably necessary to respond to a child safety concern, complaint, incident or investigation, subject to applicable legislative requirements.
- Educators must ensure that surveillance devices and associated systems are operated and maintained in a manner that minimises the risk of unauthorised access, interference or disclosure.
- Any changes to surveillance arrangements that may affect children's safety, privacy or the approved Family Day Care environment must be communicated to Service Management.
- The use of surveillance devices, including baby monitors and other monitoring technologies, does not replace an Educator's responsibility to adequately supervise children or undertake required physical checks, including safe sleep checks.

- Any concerns, complaints or incidents relating to the operation of surveillance devices or the management of recorded footage must be promptly reported to Service Management as soon as practicable, but no later than 24 hours after becoming aware of the incident, including incidents occurring outside normal office hours.

6. CHILDREN'S USE OF DIGITAL TECHNOLOGIES

Nature Alliance Family Day Care recognises that digital technologies can provide opportunities to support children's learning, development, creativity, communication and participation in educational experiences.

- Educators will ensure that children's use of digital technologies is appropriate to their age, developmental abilities, individual needs and the educational purpose of the activity.
- Digital technologies may be incorporated into the educational program where they support children's learning, development, exploration, creativity or participation.
- Educators must identify and manage risks associated with children's use of digital technologies, including exposure to inappropriate content, online interactions, privacy, security and the physical and social impacts of device use.
- Children must be appropriately supervised when using digital devices or accessing online environments, with the level of supervision determined by the nature of the activity, the technology being used and the individual needs of the child.
- Educators will take reasonable precautions to ensure that digital content, applications, websites and online resources accessed by children are safe, appropriate and consistent with the Service's child safety requirements.
- The use of digital technologies must not compromise children's opportunities for physical activity, social interaction, play, rest or engagement in other developmentally appropriate experiences.
- Children's access to digital technologies will be managed in consultation with families where appropriate, taking into consideration individual needs, family preferences and relevant educational or developmental considerations.
- Children are not generally permitted to use personal digital devices while attending Family Day Care. Exceptions may be considered where the use of a device supports an identified medical, disability-related, developmental or educational need, including school-related activities, subject to appropriate arrangements and safeguards.
- Where children bring personal digital devices into the Family Day Care environment, Educators must ensure their use is appropriately managed to protect the safety, privacy and wellbeing of all children in care.
- Children must not use digital devices to take, access or share images or videos of other children without appropriate authorisation and supervision.
- Educators will support children to develop an age-appropriate understanding of digital safety, respectful online behaviour, privacy and the responsible use of technology.

7. DIGITAL SAFETY, PRIVACY & SECURITY

Nature Alliance Family Day Care is committed to protecting children's safety, privacy and personal information when using digital technologies and online environments.

The Service will maintain appropriate safeguards to minimise risks associated with the collection, access, use, storage and disclosure of digital information, including images and videos of children.

- Educators, staff and other authorised persons must use digital technologies and online environments in a manner that protects the safety, privacy, dignity and confidentiality of children and families.
- Digital information relating to children and families must only be accessed, used or disclosed for legitimate and authorised purposes, in accordance with applicable legislation and Service policies.
- Appropriate measures must be implemented to protect digital devices, applications, accounts and information from unauthorised access, misuse, loss or disclosure.
- Educators and staff must use Service-authorised systems and arrangements when collecting, storing or sharing children's personal information, including images and videos.
- The suitability and potential risks of digital applications, online platforms and connected technologies must be considered before their use in connection with the education and care of children.
- Children's personal information, images or videos must not be entered into, uploaded to or processed through unauthorised digital platforms or artificial intelligence applications.
- Digital information and records must be managed in accordance with the Service's Data Security Policy, Social Media Policy and relevant confidentiality, privacy and recordkeeping policies.

8. RESPONDING TO DIGITAL SAFETY INCIDENTS & BREACHES

Nature Alliance Family Day Care is committed to responding promptly and appropriately to concerns, incidents or breaches involving digital technologies and online environments, with children's safety, wellbeing and privacy remaining the priority.

- Educators, staff and other relevant persons must promptly report to Service management any actual or suspected incident involving the unsafe, inappropriate or unauthorised use of digital technologies, including concerns relating to children's images, videos, personal information or online safety.
- Where an incident or concern is identified, immediate and appropriate action must be taken to protect children from further harm and minimise any ongoing risks.
- A written record of the incident, including the circumstances and immediate actions taken, must be completed and forwarded to Service management as soon as practicable, but no later than 24 hours after becoming aware of the incident.
- Service management will assess reported incidents and determine an appropriate response, having regard to the nature and seriousness of the concern, potential risks to children and any applicable legislative requirements.
- Appropriate steps must be taken to preserve relevant information or evidence, prevent further unauthorised access, use or disclosure, and support any necessary investigation.
- Incidents will be documented and managed in accordance with the service's relevant policies and procedures, including those relating to child protection, complaints, privacy, confidentiality and data security.
- Where required, the Service will notify the Regulatory Authority, relevant government agencies, law enforcement authorities or other appropriate bodies in accordance with applicable legislative and reporting obligations.

- Parents and guardians will be informed of incidents affecting their child where appropriate and in accordance with relevant legislative requirements, having regard to the child's safety, privacy and any investigation or reporting obligations.
- The Service will review incidents and implement any necessary corrective actions, including changes to risk management arrangements, device authorisations, practices or procedures, to minimise the likelihood of recurrence.

Sources
Office of the Australian Information Commissioner (OAIC)
Child Care Centre Desktop
Privacy Act 1988 (Cth) and Australian Privacy Principles, where applicable
National Principles for Child Safe Organisations
National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care, as reflected in applicable legislation and regulatory requirements

Supporting Policies.
NA-POL-1.6 Child Protection
NA-POL-001.7 Child Safe Environment
NA-POL-0007 Confidentiality, Privacy and Educator Record Management
NA-POL-0011 Participation of Volunteers and Students on Practicum Placements
NA-POL-0032 Social Media
NA-POL-37 Service Confidentiality, Privacy, Record Keeping and Retention Policy
NA-POL-0039 Data Security