Safe Use of Digital Technologies and Online Environments

1. Statement

NBCA ensures the safe, ethical, and responsible use of digital technologies and online environments to protect the privacy, wellbeing, and developmental needs of children. NBCA sets clear expectations for the use of digital devices, images, videos, artificial intelligence, and optical surveillance systems, and upholds a commitment to data security, child safety, and legal compliance. All digital practices are designed to support high-quality education and care while safeguarding personally identifiable and sensitive information.

2. Definitions

“Approved Provider” means an entity operating a childcare service or services and to which all obligations and liabilities of the service are attached; at NBCA, the Approved Provider is the President of the Management Committee, or any other member of the Management Committee in the absence of the President.

“Authorisation” means formal, documented permission given by a person with appropriate authority under NBCA’s policies. This may include consent from a parent/guardian, such as image consents on an enrolment form or an image release, or written approval from the Approved Provider.

“Biometric data” means information derived from an individual’s biological or behavioural characteristics, such as facial recognition or fingerprints, that can be used to identify them.

“Cloud-based systems” means online platforms used for data storage, communication, or educational content delivery, including third-party apps, portals, or learning management systems.

“Data breach” means an incident where confidential or proprietary information is lost or accessed, disclosed, or otherwise dealt with in an unauthorised way. This includes cyberattacks, device theft, or accidental sharing.

“Digital devices” means any electronic device capable of storing, accessing, transmitting, or processing data. This includes, but is not limited to, desktop computers, laptops, tablets, mobile phones, smartwatches, cameras, and any other internet-connected or data-enabled technology used for communication, documentation, administration, or learning purposes within the service.

“Personally identifiable information” means any information that can be used to identify an individual, either directly or indirectly. This includes names, contact details, images, videos and other identifying data. Personally identifiable information may also include sensitive information, which is subject to additional protections under Australian privacy law.

“Under control of the service” means the platform or tool is formally approved by NBCA, with NBCA retaining administrative control and ensuring appropriate privacy, security, and access controls are in place.

3. Taking, use, storage and destruction of images and videos of children

i. Parent/guardian authorisation to take, use, and store images and videos of children is sought at enrolment and reconfirmed each year while the child attends an NBCA service. Authorisation may be refused, withdrawn, or limited at any time by providing written notice to the Responsible Person.

ii. In the absence of valid authorisation, NBCA will take all reasonable steps to ensure that no identifiable images or videos of a child are taken, used, or stored. However, images and videos may be taken, used and stored without authorisation where required or authorised by law, including for incident reporting, child protection obligations, legal proceedings, or compliance with regulatory requirements.

iii. Where authorised, services take, use and store images and videos to support children's learning, development, and wellbeing. This documentation enables educators and teachers to reflect on practice, plan responsive curricula, engage families in their child's learning, and maintain high-quality educational and care environments.

iv. Images and videos of children are taken in the context of their day-to-day experiences at the service. This may include individual and group learning activities, play-based interactions, daily routines, and participation in events, incursions, and excursions.

v. Images and videos of children are only taken in appropriate, non-private settings. They are never taken in toilets, nappy changing areas, during rest or sleep periods, or during personal care routines, even if requested or authorised by parents/guardians.

vi. Images and videos of children will not be used for external purposes – including social media, marketing, or publications – without specific written authorisation from parents/guardians. Where authorisation is given, NBCA takes all reasonable steps to protect children's privacy by avoiding identifiable facial images and excluding any personal or enrolment information.

vii. NBCA stores images and videos in secure, cloud-based systems, some of which may be hosted on servers located outside Australia. NBCA takes all reasonable steps to assess the privacy practices and data security protocols of third-party service providers, to ensure data is protected from unauthorised access or disclosure, and that overseas data transfers are consistent with privacy principles and requirements under Australian law. Access to stored images and videos is restricted to authorised staff members who require it for approved purposes, in line with their role and responsibilities.

viii. Staff must not use any artificial intelligence tools to process or generate content using images, videos, audio, biometric data, or any personally identifiable information about children. General or de-identified prompts may be used with artificial intelligence tools under the control of the service, provided no personally identifiable information relating to children, families, or staff is included.

ix. NBCA retains images and videos in accordance with its obligations under relevant legislation, including statutory requirements for education and care services, privacy, and child protection. General images and videos of children that do not form part of a required record (e.g. incident report, educational portfolio, or mandatory documentation) will be permanently deleted within three months after the end of the calendar year in which they were captured.

4. Use of digital devices by staff and children

i. Staff must use only service-issued digital devices when accessing, storing, transmitting, or managing any information relating to children, whether they are working directly with children or in a non-contact capacity, or working on-site or remotely. Personal devices must not be used for any child-related tasks, including communication, documentation, or access to NBCA systems. This requirement ensures that all child-related work is carried out using NBCA's secure digital devices and within NBCA's monitored online environment, and complies with our legal obligations around privacy, confidentiality, and data security. For the purposes of this policy, information relating to children includes, but is not limited to:

   a. Images or videos in which a child is identifiable or mentioned, including the capture, access, use, or distribution of such content;

   b. Personally identifiable information such as a child's name, date of birth, or enrolment details;

   c. Health-related information, including medical conditions, allergies, injury records, or medication requirements;

   d. Educational documentation, including observations, assessments, notes on learning, participation, interests, or developmental progress.

ii. An exception to 4.i may apply in an emergency, where the use of a personal device is both necessary and reasonable to protect a child's safety or wellbeing, or where urgent communication or collection of child-related information is required to comply with legal or regulatory obligations.

iii. Personal digital devices may only be used by staff during designated breaks, and only where such use does not occur in the presence of children. All use must comply with NBCA policies on privacy, confidentiality, and conduct. Written authorisation from the Approved Provider is required for any exception to this clause, which will only be granted where a clear operational or personal need exists, and no material risk is posed to child safety, privacy, or compliance.

iv. All service-issued devices are subject to monitoring and are equipped with security measures to prevent unauthorised access or misuse. These include PINs, remote wipe capabilities, app usage restrictions, and managed configurations. Staff must not attempt to override or disable any security settings.

v. Staff working directly with children are expected to use digital devices and online environments in a way that supports their professional responsibilities without interfering with their supervision of children or engagement in education and care. Digital device and online environment use must be purposeful, limited to essential tasks, and never detract from the quality of interactions or safety of children.

vi. All lost or stolen digital devices, suspected data breaches, or instances of device misuse must be reported immediately to the Approved Provider. Staff must cooperate with any internal investigation and follow NBCA's data security and incident response procedures.

vii. Children may only access digital devices and online environments in open, supervised environments under direct supervision. Digital devices must be set to Guided Access mode or otherwise restricted to ensure access only to approved, age-appropriate content.

viii. Any digital or online experiences offered to children must be developmentally appropriate, linked to planned learning outcomes, and support and extend children's learning in meaningful ways. Technology must only be used to enhance learning, never as a form of reward.

5. Use of optical surveillance devices

i. NBCA services use 24-hour, motion-activated closed-circuit television (CCTV) for optical surveillance. These systems record video footage only and do not capture audio.

ii. Optical surveillance is used for the safety and protection of children, families, staff, and visitors, and to support the prevention, detection, and investigation of incidents involving unlawful conduct, breaches of regulatory obligations, injury, and property damage.

iii. Optical surveillance applies to all individuals on the premises, including children, families, staff, and visitors. Optical surveillance devices are installed in visible locations, with signage clearly identifying all areas under surveillance.

iv. Optical surveillance in services is designed to be proportionate to the need for safety and protection, while minimising intrusion. Devices are not installed in toilets, nappy changing areas, or other spaces where children, families, staff, or visitors may reasonably expect privacy.

v. Access to optical surveillance systems and recorded footage is limited to authorised personnel with a clear operational need. Access is granted only where necessary for legitimate purposes, such as investigating incidents, ensuring safety and security, fulfilling legal or regulatory obligations, or supporting internal reviews.

vi. Footage is accessible for a defined period based on system capacity, after which it is automatically overwritten. Where required for safety, legal, or compliance purposes, relevant footage will be extracted, securely stored, and retained in accordance with NBCA's data management procedures and applicable legal obligations.

EFFECTIVE DATE	1 September 2025	**LAST REVIEWED**	August 2025

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2	Safety	Each child is protected
2.2.1	Supervision	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.

2.2.2	Incident and emergency management	Plans to effectively manage incidents and emergencies are developed in consultation with relevant authorities, practised and implemented.
2.2.3	Child protection	Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect.
QUALITY AREA 5: RELATIONSHIPS WITH CHILDREN		
5.1.1	Positive educator to child interactions	Responsive and meaningful interactions build trusting relationships which engage and support each child to feel secure, confident and included.

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS

S. 165	Offence to inadequately supervise children
S. 167	Offence relating to protection of children from harm and hazard
S. 175	Offence relating to requirement to keep enrolment and other documents
84	Awareness of child protection law
155	Interactions with children