



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

POLICY STATEMENT

BDCS is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and the wider community. Digital technologies have become an integral part of many children's daily lives and we recognise that they can have a number of benefits. However, children's safety is always our priority, and it is imperative that personal and work technological devices are used appropriately in order to protect children from any potential harm.

BACKGROUND

As a child safe organisation, BDCS embeds the National Principles for Child Safe Organisations and continuously addresses risks to ensure children are safe in physical and online environments. Children's safety and wellbeing is paramount, and our organisation has the responsibility 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 BDCS philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, staff and families. Children have the right to be protected from the misuse of images and videos whilst at BDCS and we have therefore adopted all of the guidelines in [The National Model Code - Taking Images or Videos of Children while providing Early Childhood Education and Care](#).

This policy applies to all children, families, staff, management, contractors, students, volunteers and visitors of our services. Any breach in this policy may result in disciplinary action, police involvement, or termination of access to any of our services.

OVERALL STRATEGIES / HOW WILL IT BE DONE?

Our organisation uses digital technology and electronic devices as a tool for learning with children, documenting their learning and development, communicating with families and the wider community, supporting program planning and administration tasks, promoting the learning that occurs within our services and enhancing safety and security through systems such as sign in/out platforms and CCTV monitoring.

We recognise that taking images or videos of children while in attendance at our services can have many benefits including, allowing educators to track their progress and to in turn, share this progress with their families. In order to protect children's safety, this policy outlines the conditions that must be adhered to when taking images or videos of children at our services.

THE NATIONAL MODEL CODE - TAKING IMAGES OR VIDEOS OF CHILDREN WHILE PROVIDING EARLY CHILDHOOD EDUCATION AND CARE

Our organisation has adopted the National Model Code and Guidelines for taking images or videos of children. The National Model Code sets out recommended child safe practices for taking, sharing and storing images or videos of children while providing early childhood education and care. The recommended practices are set out in four parts of the National Model Code, which outline:

- Only service-issued electronic devices should ever be used to take images or record videos of children
- Personal electronic devices that can take images or record images should not be carried while providing ECEC, except for authorised essential purposes
- Considerations for why someone may need to continue to carry a personal electronic device that can take or record images (authorised essential purposes)
- The need for strict controls for storing and retaining images or recordings of children

The National Model Code continues to apply when providing Early Childhood Education and Care outside a service's premises. This could include during excursions or regular outings, or when a child is transported by the service.

ONLY SERVICE-ISSUED ELECTRONIC DEVICES SHOULD EVER BE USED TO TAKE IMAGES OR RECORD VIDEOS OF CHILDREN

- Parents/guardians must provide written notification regarding whether they consent to:
 - Their child being photographed/videoed by BDCS



QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- Any images/videos of their child being displayed in any BDCS service
- Any images/videos of their child being uploaded to the service approved online platform (Xplor/Storypark) which will enable educators to share observations with the child's parents/guardians and other children's families
- Any images/videos of their child to be published by BDCS (e.g. website/social media/BDCS documentation)
- Any images/videos of their child to be shared with any outside agencies (e.g. an agency who visited for an incursion) or used by students as part of their placement
- The above written notifications are initially completed as part of the child's enrolment form but can be updated at any time by notifying the relevant service in writing.
- BDCS will only ever intentionally photograph/video children whose parent/guardian has given consent. If photo or video consent is not provided, a child may still be included in group or candid moments; however, BDCS will ensure their face is not visible in any shared content.
- Should a child's face unintentionally appear in a photo/video, this will not be shared with anyone and deleted as soon as practicable.
- BDCS strictly does not allow for any inappropriate images/videos to ever be taken. Inappropriate images/videos are any that are not directly relevant to the child's participation in the activities of the service. Examples of inappropriate (and potentially illegal) images or videos include where a child is:
 - Not appropriately dressed, for example, in their underwear, in a state of undress, completely undressed or with their genitalia exposed
 - In a position that could be perceived as sexualised in nature
 - In distress or anxious/experiencing or demonstrating distress or dysregulation.
- There are also certain locations where BDCS prohibits images/videos to be taken. These include:
 - In bathrooms and nappy change areas
 - Cot rooms
 - Any space where two educators are unable to see everything that is happening, including the image/video being taken
- Only BDCS devices will be used to photograph/video children who are in attendance at any of our BDCS services.
- All BDCS devices are clearly labelled with the BDCS logo on the back of the device and on the home/lock screen to make for easy identification.
- BDCS devices must not be removed from the premises without prior permission from the Approved Provider/Nominated Supervisor due to the confidential information that is stored on them. BDCS has systems in place to ensure that this information is kept secure even when the device leaves the premises (more information available in 'Engagement of a Managed IT Service section).
- Any staff member or verified contractor can take an image/video using a BDCS device (not students, volunteers or visitors). Consideration will always be given to the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.
- We understand that students may need to take images/videos while at the service as evidence of their placement. We do not permit students to use their own devices to do this. Instead, they can request their BDCS supervisor to use a BDCS device to do this and the images/videos will then be appropriately shared with the student.
- An asset register is maintained which lists all BDCS technological devices and relevant details such as the device type, the registered user (if applicable) and the specific number provided by the external IT services which enables them to have full control and ensure all security features remain current.
- All BDCS devices are password protected and only staff members and verified contractors know the password.
- 'No photography/videography' signs are displayed on the gates to our services informing families/visitors that they are not allowed to take images or record videos whilst on our service premises.
- Should a parent/guardian ever wish to take an image/video of their child whilst at the service, they are encouraged to ask a BDCS staff member who will take the image/video on a BDCS device and then share this with the family via the online platform used by the service to share observations of children.



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- We recognise that at times, other agencies may wish to take images/videos of children for their own purposes e.g. a local dance group providing an incursion may wish to take and share images for promotional purposes. In this situation, the outside agency can request for BDCS to take images/videos on a BDCS device and for these to be appropriately shared with the outside agency.
- All aspects of the Safe Use of Digital Technologies and Online Environments policy will be adhered to when sharing images/videos with outside agencies, including students. The staff member who shares the images/videos is responsible for ensuring that only images/videos of children with the appropriate consent is shared.
- When children are on an excursion from the service, the excursion coordinator will inform those involved with organising the excursion that they must not take images/videos of the children. BDCS staff will also be vigilant of members of the public who may attempt to take images/videos of the children and request that they not do this.
- Parents/guardians must understand that if they consent to their child going on an excursion, there is the possibility that they will be photographed/videoed by members of the public despite BDCS strongly discouraging this.

PERSONAL ELECTRONIC DEVICES THAT CAN TAKE IMAGES OR RECORD IMAGES SHOULD NOT BE CARRIED WHILE PROVIDING ECEC, EXCEPT FOR AUTHORISED ESSENTIAL PURPOSES

- BDCS does not allow any personal technological devices (such as laptops, tablets, phones, cameras, and smart watches with cameras and META sunglasses) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) to be carried by any staff member, contractor, student or volunteer while providing Early Childhood Education and Care.
- Any exceptions to this should be for limited, essential purposes that are authorised in writing (or through another means if written authorisation is not reasonably practicable) by the Approved Provider/Nominated Supervisor, and where that access does not impede the active supervision of children.
- BDCS devices are issued to those who require them and are managed by an external IT service who ensure that all confidential information including images/videos, is kept secure. The IT service will ensure that this information can only be accessed by relevant persons and monitored to ensure that it is being used for work purposes only.

CONSIDERATIONS FOR WHY SOMEONE MAY NEED TO CONTINUE TO CARRY A PERSONAL ELECTRONIC DEVICE THAT CAN TAKE OR RECORD IMAGES (AUTHORISED ESSENTIAL PURPOSES)

- Essential purposes for which use and/or possession of a personal electronic device may be authorised for purposes other than taking images or recording videos of children include:
 - Communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
 - Personal health requirements, e.g. heart or blood sugar level monitoring
 - Disability, e.g. where a personal electronic device is an essential means of communication
 - Family necessity, e.g. a staff member with an ill or dying family member
 - Technology failure, e.g. when a temporary outage of service-issued electronic devices has occurred
 - Local emergency event occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification
- The Approved Provider/Nominated Supervisors will ensure ongoing monitoring and review of any authorised use of a personal electronic device to ensure use of the device is consistent with what is permitted, and the authorisation remains current.

AUTHORISATION FOR CARRYING A PERSONAL ELECTRONIC DEVICE

- It is at the discretion of the Approved Provider/Nominated Supervisor whether to authorise this request.
- Should this written request be authorised, a written response will be provided which will include details of how long this authorisation is in place for and whether there are any restrictions in place.
- Should the authorisation need to be extended, the process is to be repeated, and a new written request is to be submitted.

THE NEED FOR STRICT CONTROLS FOR STORING AND RETAINING IMAGES OR RECORDINGS OF CHILDREN



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- Images/videos of children can only be accessed by authorised BDCS staff members and verified contractors, as determined and monitored by the Nominated Supervisors and the Approved Provider.
- All images/videos are securely stored on BDCS devices which are all password protected and only accessible by BDCS staff members and verified contractors.
- All images/videos are backed up on BDCS cloud storage and SharePoint which is password protected and only accessible by authorised BDCS staff members and verified contractors.
- Secondary storage devices are never permitted to be used to store images/videos or any other information in relation to children.
- Images/videos of children can be stored for up to 10 years after a child's enrolment ceases and then all copies of the image/video are permanently removed from all devices and cloud storage.
- Provided consent has been given, each child will have a profile on an online educational platform which will enable educators to share observations (including images/videos) with families. The child's profile will remain for up to 10 years after a child's enrolment ceases, at this point the profile is permanently deleted.
- A written request for any images/videos which have been published by BDCS on a BDCS platform, to be removed can be made at any time by a child's parent/guardian. Any images/videos which have been shared with any outside agencies are no longer the property of BDCS and therefore BDCS has no control over how they are shared or stored.

INAPPROPRIATE SHARING OF IMAGES OR VIDEOS

It is inappropriate for an image or video of a child to be shared to platforms beyond the intended educational purpose of the image or video. Any image or video recording of a child can become inappropriate if shared in the wrong context or for an unintended purpose. This includes if an individual transfers images to their own account or device either directly or via the cloud, for example, to post images or videos on social media or other applications/software platforms that were not its intended purpose.

BDCS has strict systems in place to ensure that no images or videos can be transferred from a BDCS devices to a personal device. Should BDCS discover that the inappropriate sharing of images or videos have occurred, the person/persons involved may face disciplinary action, police involvement, or termination of access to any of our services.

ENGAGEMENT OF A MANAGED IT SERVICE

Our organisation has engaged a managed IT service to provide maintenance, monitoring, restoration and support for all BDCS technological devices with a goal to regularly look to improve cybersecurity practices. This ensures that there are secure systems in place to prevent any BDCS devices from being used inappropriately. Our organisation is actively upgrading its IT and security maturity through:

- Microsoft 365 Business Premium rollout
- Multi-layered security (MFA, threat protection, geo-blocking, email backups, and signature management)
- Endpoint protection upgrade
- Mobile device and firewall alignment
- Hardware review and OS standardisation
- Essential 8 practices (Application whitelisting, managed domain protection)
- Risk monitoring and incident restoration
- Full mobile device management
- Back-up solutions

ACCESS TO BDCS SOFTWARE

BDCS uses a range of software programs and apps on BDCS devices to support the educational program and administration of the organisation. All programs and apps used are carefully selected with consideration given to their levels of security and they are kept up to date with the latest available system updates.

- Access to software programs and apps are password protected and monitored by BDCS on a frequent basis.



QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- The Approved Provider will ensure programs which require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law.
- Staff members are unable to access any software used by BDCS on any of their personal devices. For those staff members needing to access BDCS software, they will be provided access to a BDCS device to use.

USE OF TECHNOLOGY BY CHILDREN

Technology when used appropriately, can be a tool for learning, especially when educators play an active role in assisting children to use technology competently and safely. As part of our enrolment form, parents/guardians are asked if they consent to their child being able to use/view technology for curriculum enhancement purposes only.

Our services will promote responsible behaviours and limit screen time when using technology by never exceeding the recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines. Technology will only be used by children as an extension to the daily program, assisting in the development of social, physical, emotional, cognitive, language, and creative potential of each child. Educators and the technology that they use will always remain in line-of-sight of other staff members when working with children.

All educators are diligent in ensuring that children are only able to access age-appropriate technology on BDCS devices. Educators will exercise appropriate judgement and behave in a professional and ethical manner when using technology. At all times, educators will provide a child safe environment and directly supervise children when using technology to minimise the opportunity for abuse or other harm to occur.

In addition, educators will inform children that if they encounter anything unexpected online that makes them feel uncomfortable, scared or upset, whether it be at or away from the service, they can seek support from any educator.

CLOSED-CIRCUIT TELEVISION SYSTEM (CCTV)

Our organisation operates Closed-Circuit Television System (CCTV) to ensure the health, safety and protection of children, staff, families and visitors. BDCS adheres to the Privacy Act 1988 and complies with the Australian Privacy Principles. We will regularly review guidance on the use of surveillance devices, including information provided by the Office of the Australian Information Commissioner.

CCTV USE

- Specific camera locations will vary across the BDCS sites and outdoor security cameras may cover:
 - Building entrances
 - Premises gates
 - Carparks
 - Outdoor areas
- Cameras will never be placed in or be able to reach any of the following locations:
 - Toilets
 - Change rooms
 - Bathrooms and showers
 - Breastfeeding locations
 - Areas put aside for prayer
 - Staff rooms
- Outdoor security camera footage is used for security and is not continuously monitored.
- 'Eufy Security' is the system that is used and the account to review footage can only be accessed by staff members authorised by the Approved Provider.
- The correct time and date will always be set on each of the cameras.
- All cameras are clearly visible, and signage is displayed at the entrance to each service to notify the public that they are entering a site with security cameras, with audio recording capabilities in use.
- All staff and families are notified about the surveillance devices at the service including:



QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- The kind of surveillance to be carried out (camera, computer, or tracking)
- How the surveillance will be carried out
- When the surveillance will start and if it will be continuous or intermittent
- Whether the surveillance will be for a specified limited period or ongoing
- Who has access to the footage
- How and when the footage will be deleted

MONITORING AND STORAGE

The CCTV recording system operates in real mode, monitoring the site continuously 24 hours a day, some images may be recorded (whether they are monitored or not). Such records may be accessed and used for investigative, training or evidentiary purposes. The duration of time that recorded images are held will vary from services to service due to variables including the use of motion sensing technology and the size of storage devices. Generally, recorded images are held for between 30 and 60 days (unless a copy is made for the purposes of an ongoing investigation, as evidence of a security concern or incident, complying with a relevant law). After that time footage is deleted or de-identified in accordance with relevant laws.

Footage and information collected via the recording system will be governed by Australian Privacy Principles and all relevant staff will be kept up to date with requirements under Australia's privacy law (there are some Commonwealth, State and territory laws that restrict the use of listening, optical, data and tracking surveillance devices).

Access to CCTV footage is strictly controlled and protected by secure, password-protected systems. Only authorised personnel are permitted to access the footage, in accordance with privacy laws and BDCS policies. The Approved Provider is responsible for determining who is authorised to access CCTV footage. Any requests to view CCTV footage will be managed in accordance with Australian Law and access to the recordings will only be disclosed to:

- The Ombudsman (NSW) to assist with investigations on 'child protection' (e.g. abuse, neglect and ill treatment).
- To a member or officer of a law enforcement agency e.g., Police for use in assisting with investigations.
- The Approved Provider, Nominated Supervisor or Responsible Person on duty to investigate situations that may have occurred.

PRIVACY AND CONFIDENTIALITY

Our Privacy and Confidentiality Policy applies at all times, including when using digital technology and accessing online environments. Any information, images, or digital content related to children, families, and the organisation is collected, stored, used, or shared in accordance with privacy legislation and BDCS procedures, to maintain confidentiality and protect the safety and wellbeing of children. The Approved Provider must be notified as soon as possible regarding any potential threat to security information and access to data sensitive information.

The Approved Provider will notify the Office of the Australian Information Commissioner (OAIC) in the event of a possible data breach by using the online [Notifiable Data Breach Form](#). This could include:

- A device containing personal information about children and/or families is lost or stolen.
- A data base with personal information about children and/or families is hacked.
- Personal information about a child is mistakenly given to the wrong person.

BREACH OF POLICY

- Any staff member who fails to adhere to any aspect of this policy may be in breach of their terms of employment and may receive disciplinary action including termination and/or police action may be taken.
- Students, volunteers or visitors who fail to comply with this policy may face termination of their engagement with the service and/or police action may be taken.
- Families who fail to comply with this policy may be asked to leave the premises and/or police action may be taken. In addition, families are to ensure that their children do not bring any technology or personal storage and file transfer media into the service. Any breach in this may result in the technology or personal storage and file transfer media



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

being removed from the child by a staff member and securely stored and returned to the parent/guardian or authorised nominee when the child departs the service.

WHAT TO DO IF THIS POLICY IS NOT BEING ADHERED TO

Child safety is everyone's responsibility. Should any child, family member, staff member, contractor, student, volunteer or visitor suspect that this policy is not being adhered to, they should immediately report this concern to the Responsible Person/Nominated Supervisor of the service or the Approved Provider as per the Complaints Handling policy.

COMPLAINTS TO THE REGULATORY AUTHORITY

In addition, as per our Complaints Handling policy, any complaint can be made directly to the Regulatory Authority where the complaint alleges that:

- The safety, health or wellbeing of a child or children was or is being compromised while that child or children is or are being educated and cared for by the approved education and care service.
- The relevant legislation has been contravened.

Complaints can be submitted via:

Email: ececd@det.nsw.edu.au

Post: Early Childhood Education Directorate, NSW Department of Education, Locked Bag 5107, Parramatta, NSW 2124

Phone: 1800 619 113

REPORTING

MANDATORY REPORTER REQUIREMENTS

Staff, contractors who work directly with children, students and volunteers are reminded that they are Mandatory Reporters and should they have reasonable grounds to believe that a child is at risk of significant harm, they are required to report this as per our Child Protection Policy. Mandatory Reporters should use the Mandatory Reporters Guide to determine whether a report to the Department of Communities and Justice (DCJ) Child Protection Helpline is required.

Any person in the community who has reasonable grounds to believe that a child is at risk of significant harm can also report to the Department of Communities and Justice (DCJ) Child Protection Helpline.

Department of Communities and Justice (DCJ) Child Protection Helpline:

Phone: 132 111 (this is a 24-hour service).

ADDITIONAL REPORTING REQUIREMENTS

The Nominated Supervisor must ensure that:

- Any suspected cases of online abuse are reported to the relevant authorities, including the eSafety Commissioner and Police, in accordance with legal requirements and child protection procedures.
- A notification is made to the Regulatory Authority within 24 hours via the [NQA-ITS](#), if a child is involved in a serious incident, including any unsafe online interactions, exposure to inappropriate content, or suspected online abuse.

USEFUL RESOURCES

Australian Children's Education & Care Quality Authority. [National Model for Early Childhood Education and Care](#)

[Australian Government Office of the eSafety commission](#)

[eSafety Early Years Program for educators](#)

[eSafety Early Years Program checklist](#)

[eSmart Alannah & Madeline foundation](#)

[Family Tech Agreement. eSafety Early Years Online safety for under 5s](#)

Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content:

<https://www.kiddle.co/>

Office of the Australian Information Commissioner (OAIC)

ROLES AND RESPONSIBILITIES

THE APPROVED PROVIDER, NOMINATED SUPERVISORS AND OTHER BDCS MANAGEMENT WILL:

- Ensure that obligations under the Education and Care Services National Law and National Regulations are met.



QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- Ensure all staff (including casual staff) receive information and induction training to fulfil their roles effectively, including being made aware of the Safe use of Digital Technologies and Online Environments Policy, their responsibilities in implementing it, and any changes that are made over time.
- Ensure students, visitors and volunteers have knowledge of and adhere to this policy.
- Ensure all staff, volunteers and students are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children.
- Ensure all contractors have knowledge of and adhere to this policy.
- Create a list of 'Verified Contractors' for the purpose of this policy, who have access to BDCS devices and software.
- Ensure the National Principles for Child Safe Organisations is embedded into the organisational structure and operations.
- Ensure the National Model Code guidelines are understood by all staff, approved contractors, students and volunteers and adopted within the organisation.
- Ensure children's safety is maintained at all times and their right to privacy respected.
- Develop and monitor an Electronic Device Register for all electronic devices purchased and used at the services.
- Ensure that taking images/videos of children is risk assessed in the Child Safe Risk Management Plan.
- Ensure parents/guardians are informed of how the BDCS will take, use, store and destroy images and videos of children enrolled at the service.
- Clearly display posters stating that images/videos must not be taken while on the premises unless taken on a BDCS device by a BDCS staff member.
- Ensure families and visitors understand the reason for our rules regarding photography/videography and the positive impact this has on supporting children's safety.
- Ensure enrolment forms are completed accurately and that appropriate records are made of exactly who has consent to be photographed/videoed and the circumstances regarding when these images/videos can be shared.
- Ensure enrolment information remains accurate and is shared with relevant staff only.
- Ensure sensitive information about a child's full name, address, date of birth etc. or any other information that reveals their identity is never published.
- Ensure that separate written permission is obtained from parents/guardians for their child to be photographed when an outside photographer is contracted to take annual individual and group images. Only children who have written permission from their parent/guardian will be included in this photography.
- Ensure staff, children and families are aware of our complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter.
- Ensure the Privacy and Confidentiality Policy is adhered to at all times.
- Ensure digital data is stored securely.
- Ensure policies and procedures are reviewed following an identification of risks following the review of risk assessments relating to the use of digital technologies and online environments.

ALL STAFF, VERIFIED CONTRACTORS, STUDENTS AND VOLUNTEERS WILL:

- Ensure they promote and support a child safe environment, ensuring adherence to the Child Safe Environment and Child Protection Policies, including mandatory reporting obligations.
- Understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe.
- Ensure every child in their care is protected from any exploitation of images/videos of themselves taken whilst in attendance at the service.
- Be vigilant when visitors are on site and positively inform/remind them about the BDCS commitment to creating a child safe culture and that they mustn't take any images or videos at any time whilst on the premises.
- Ensure any images/videos are taken for a suitable purpose, including to:
 - Support the individual learning of each child for their formal record
 - Record children's work and activities within the service environment
 - Be used for promotional purposes by BDCS or outside agencies



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

- Ensure that the supervision of children and their safety is always the main priority and that taking images/videos of children doesn't negatively impact the supervision that they provide.
- Ensure that children participate in decisions affecting them including providing permission to have images/videos taken of them.
- Not use, or have access to, any personal electronic devices while working directly with children.
- Keep passwords confidential and log out of technology and software programs after each use.
- Ensure sensitive information about a child's full name, address, date of birth etc. or any other information that reveals their identity is never published.
- Ensure that screen time is not used as a reward or to manage challenging behaviours under any circumstances.
- Introduce concepts to children about online safety at age-appropriate levels by providing age-appropriate guidance, discussions and activities that help them to recognise safe and unsafe online behaviours.
- Consult with children about matters that impact them, including the use of digital technologies and online environments, to ensure their voices are heard and respected in a meaningful way.]

FAMILIES AND VISITORS WILL:

- Act in accordance with this policy at all times and comply with BDCS' adoption of the National Model Code.
- Understand that any non-compliance with this policy may result in them being asked to leave the service.
- Not use personal electronic devices for any reason including to take any images/videos at any point whilst on BDCS premises where children are present, except to sign their child in/out of the service via the Xplor app.
- Accurately complete their child's enrolment form and inform the relevant service in writing if there are ever any changes to the consent that they have provided regarding:
 - Taking and sharing images/videos of their child
 - Their child being able to use/view technology for curriculum enhancement purposes
- Understand that if photo/video consent is not provided, their child may unintentionally appear in images/videos however, BDCS will ensure that their face is not visible in any shared content. Should a child's face unintentionally appear in an image/video, this will not be shared with anyone and will be deleted as soon as practicable.
- Be requested to provide written permission for any professional photography that may occur at the service.
- Understand that if they consent to their child going on an excursion, there is the possibility their child will be photographed/videoed by members of the public despite BDCS strongly discouraging this.

CONTINUOUS IMPROVEMENT/REFLECTION

Our Safe use of Digital Technologies and Online Environments Policy will be reviewed on an annual basis in consultation with children, families, staff and management. If there are any incidents in relation to this policy, it will be reviewed immediately.

CHILD SAFE STANDARDS

Standard 1	Child safety is embedded in organisational leadership, governance, and culture
Standard 2	Children participate in decisions affecting them and are taken seriously
Standard 3	Families and communities are informed and involved
Standard 5	People working with children are suitable and supported
Standard 8	Physical and online environments minimise the opportunity for abuse to occur
Standard 10	Policies and procedures document how the organisation is child safe

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDRENS 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
2.2.3	Child Safety and Protection (effective Jan 2026)	Management, educators and staff are aware of their roles and responsibilities regarding child safety, including the need to identify and respond to every child at risk of abuse or neglect

QUALITY AREA 5: RELATIONSHIPS WITH CHILDREN



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

5.1.2 Dignity and rights of the child The dignity and rights of every child are maintained

QUALITY AREA 6: COLLABORATIVE PARTNERSHIPS WITH FAMILIES AND COMMUNITIES

6.1.2 Parent views are respected The expertise, culture, values and beliefs of families are respected, and families share in decision-making about their child's learning and wellbeing

QUALITY AREA 7: GOVERNANCE AND LEADERSHIP

7.1.2 Management Systems Systems are in place to manage risk and enable the effective management and operation of a quality service that is child safe

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS AND NATIONAL LAW

- Sec. 162 (a) Child protection training
- Sec. 165 Offence to inadequately supervise children
- Sec. 167 Offence relating to protection of children from harm and hazards
- 12 Meaning of serious incident
- 73 Educational Program
- 76 Information about educational program to be given to parents
- 84 Awareness of child protection law
- 115 Premises designed to facilitate supervision
- 122 Educators must be working directly with children to be included in ratios
- 123 Educator to child ratios – centre-based services
- 149 Volunteers and students
- 155 Interactions with children
- 156 Relationships in groups
- 168 Education and care service must have policies and procedures
- 170 Policies and procedures must be followed
- 171 Policies and procedures to be kept available
- 172 Notification of change to policies and procedures
- 175 Prescribed information to be notified to Regulatory Authority
- 176 Time to notify certain information to Regulatory Authority
- 181 Confidentiality of records kept by approved provider
- 183 Storage of records and other documents
- 184 Storage of records after service approval transferred
- 195 Application of Commonwealth Privacy Act 1988

STATUTORY LEGISLATION & CONSIDERATIONS

- [A New Tax System \(Family Assistance\) Act 1999](#)
- [Child Care Subsidy Secretary's Rules 2017](#)
- [Education and Care Services National Law Act 2010 \(Amended 2023\)](#)
- [Education and Care Services National Regulations \(Amended 2023\)](#)
- [Family Law Act 1975](#)
- [Privacy Act 1988](#)
- [Work Health and Safety Act 2011](#)
- [Workplace Surveillance Act 2005](#)

SOURCES

- Acknowledgement to Community Early Learning Australia and Childcare Centre Desktop.
- Australian Children's Education & Care Quality Authority (ACECQA). (2024). [Taking Images or Videos of Children While Providing Early Childhood Education and Care. Guidelines for the National Model Code.](#)
- Australian Children's Education & Care Quality Authority (ACECQA). (2023). [Embedding the National Child Safe Principles.](#)
- Australian Children's Education & Care Quality Authority (ACECQA). (2025). [NQF Online Safety Guide.](#)



BOURKE AND DISTRICT CHILDREN'S SERVICES

QUALITY AREA 2: CHILDRENS HEALTH AND SAFETY

POLICY NAME: SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

Australian Government eSafety Commission (2020) www.esafety.gov.au.

Australian Government Department of Education. (2022). [Belonging, Being and Becoming: The Early Years Learning Framework for Australia.V2.0](#), 2022.

Australian Government Department of Education.(2025). [Child Care Provider Handbook](#).

Australian Government Department of Health and Aged Care. (2021). [Australia's Physical Activity and Sedentary Behaviour Guidelines](#).

Australian Government, Office of the Australian Information Commissioner. (2019). Australian Privacy Principles: <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>.

Australian Human Rights Commission (2020). Child Safe Organisations. <https://childsafe.humanrights.gov.au/>.

Early Childhood Australia Code of Ethics. (2016).

Guide to the Education and Care Services National Law and the Education and Care Services National Regulations. (2017). (Amended 2025).

Guide to the National Quality Framework. (2017). (Amended 2025). [Guide to the National Quality Framework](#).

NSW Government, Office of the Children's Guardian Child Safe Standards (2020).

NSW Government. (2025). [Office of the Children's Guardian](#).

Revised National Quality Standard. (Amended 2023).

RELATED POLICIES

- Child Protection Policy
- Code of Conduct Policy
- Complaints Handling Policy
- Enrolment and Orientation Policy
- Family Participation and Communication Policy
- Governance and Management of the Service Policy
- Incident, Injury, Trauma and Illness Policy
- Interactions with Children Policy
- Privacy and Confidentiality Policy
- Providing a Child Safe Environment Policy
- Record Keeping and Retention Policy
- Student, Volunteer and Visitor Policy
- Supervision Policy

RELATED DOCUMENTS

- ACECQA National Model Code
- Enrolment Form

POLICY REVIEWED	NEXT REVIEW DATE	POLICY REVIEWED BY
SEPTEMBER 2025	SEPTEMBER 2026	Charlotte Parnaby
MODIFICATIONS	<ul style="list-style-type: none"> • One point edited which now states that 'sensitive' information, where children can be identified is not published and list of examples updated to reflect this 	
POLICY DEVELOPED	PREVIOUS MODIFICATIONS	POLICY AUTHORISED BY
AUGUST 2025	<ul style="list-style-type: none"> • New policy developed following changes to National Regulations effective from 1 September 2025 • CCTV policy merged into this policy 	Prue Ritchie