

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

Policy Number	P-Q2-M021	Version Number	1.00
Drafted by	Director of Education	Approved Date:	August 2025
		Review Date:	August 2026
Responsibility	The Board of Bubup Womindjeka Family and Children’s Centre Association (Inc.)		
Related Service Policies	<ul style="list-style-type: none"> ▪ Code of Conduct Policy ▪ Privacy and Confidentiality Policy ▪ Information and Communication Technology (ICT) Policy ▪ Child Safe Environment Policy ▪ Enrolment and Orientation Policy ▪ Interaction with Children 	<ul style="list-style-type: none"> ▪ Governance and Management of the Service Policy ▪ Mental Health and Wellbeing Policy ▪ Staffing Policy 	
Legislation and Standards	<ul style="list-style-type: none"> • Australian Children’s Education and Care Quality Authority (ACECQA): Resources on child protection and privacy practices for early childhood settings. • Child Protection -Department of Families, Fairness and Housing (DFFH) • Office of the Australian Information Commissioner (OAIC): Information on privacy rights and the protection of children’s data. • Australian Human Rights Commission: Guidance on safeguarding children’s rights, including privacy and safety. • Child Safe Organisations Guide (ACECQA): Reference documents and standards outlining best practices for child-safe environments. • Victorian Child Safe Standards • Education and Care Services National Regulations • The National Model Code for Taking Images or Videos of Children • National Quality Standard (QA2, QA5, QA6, QA7) 		
Sources	<p>Australian Children’s Education and Care Quality Authority (ACECQA): www.acecqa.gov.au</p> <ul style="list-style-type: none"> ▪ Victorian Early Childhood Regulatory Authority (VECRA) Victorian Early Childhood Regulatory Authority (VECRA) vic.gov.au PolicyGuidelines_SafeUseOfDigitalTechOnline_final.pdf <p>Quality Area 7: Governance and Leadership Quality Area 7: Governance and Leadership ACECQA</p> <p>Child Protection Home - DFFH Services</p> <p>Department of Education: Guidance on Using Electronic Devices in Early Childhood</p> <p>New guidance on using electronic devices in early childhood settings - Department of Education, Australian Government</p> <p>Child Safety Guide NQF Online Safety Guide_8.pdf</p>		

AUTHORISATION

This policy was adopted by the Bubup Womindjeka Family and Children’s Centre Board of Governance on the 15th of September 2025.

PURPOSE

This policy ensures the safe, respectful, and legally compliant use of electronic devices, digital technologies, and online environments, including photography and videography, in all areas of BWFCC's operations. It aligns with:

- Victorian Child Safe Standards
- Education and Care Services National Regulations
- The National Model Code for Taking Images or Videos of Children
- Relevant state and federal legislation, including privacy and child protection laws

The policy promotes a child-safe digital environment and supports the dignity, privacy, and wellbeing of all children at BWFCC

PRINCIPLES

Bubup Womindjeka Family and Children's Centre is committed to:

- taking every reasonable precaution to protect children from harm or hazard—including harm that may arise through digital technologies
- ensuring informed, transparent consent for photography and digital media use
- respecting children's right to privacy and participation
- ensuring staff are trained and competent in safe and ethical use of devices
- promoting accountability and secure digital practices

SCOPE

This policy applies to all staff, volunteers, and visitors involved with the early childhood service, including relief staff, external photographers, and others attending the programs and activities of Bubup Womindjeka Family and Children's Centre.

It includes:

- use of service-issued and personal electronic devices
- use of images and videos
- accessing or transmitting data
- online environments and communication platforms (e.g. Xplor, Microsoft Teams)
- AI Addendum

BACKGROUND

Bubup Womindjeka Family and Children's Centre recognises the powerful role that photographs, videos, and digital documentation can play in supporting and showcasing children's learning, development, and experiences. These tools, when used appropriately, contribute to reflective teaching practices, communication with families, and the celebration of children's achievements.

The use of electronic devices such as smartphones, tablets, cameras, and other digital recording tools must be carefully managed to ensure the privacy, safety, and protection of all children within our care. Unregulated or inappropriate use of such devices poses risks, including the unauthorised collection, distribution, or misuse of images, and could expose children to unsafe or inappropriate environments.

This policy reinforces our strong commitment to a child-safe culture in a digital world. It sets clear expectations for the ethical, respectful, and secure use of digital technologies and online platforms and also the growing need for clear, consistent guidelines around the use of electronic devices, photography, videography and storage of these within our service.

Bubup Womindjeka Family and Children's Centre (BWFCC) is committed to ensuring that all staff, families, volunteers, and visitors understand and follow best practices regarding the use of electronic devices and the handling of visual media. We aim to provide families with a transparent and respectful approach to digital documentation, ensuring that informed consent is obtained, data security is maintained, and ensuring every child's rights are upheld and every interaction with technology is safe, purposeful and protective.

CONSENT AND IMAGE USE:

- **Written Consent:** Before any photograph or video is taken, parents/guardians must provide written consent for their child to be photographed or filmed. Consent forms should specify the purpose and usage of the images that will be kept and will be updated annually.
- **Revocation of Consent:** Parents/guardians have the right to withdraw consent at any time in writing. Upon revocation, we will cease all future use of the child's images, any images of the child will be removed from public or digital spaces and deleted from the service's records within 3-5 working days.

PURPOSE OF IMAGES/PHOTOS:

Images and videos will only be used for educational, promotional (when approval has been provided), or documentation purposes related to the service. These may include:

- classroom activities, learning experiences, projects and curriculum.
- displays within the service showcase children's work and development.
- family newsletters or private online portals (e.g. Microsoft Teams and Xplor).
- promotional materials, but only with explicit consent from parents/guardians. photographs or videos should not be used for any commercial purposes without further consent.
- photographs or videos should not be used/published on staff/volunteer's personal social media platforms

INAPPROPRIATE TAKING AND SHARING OF PHOTOS/VIDEOS

Inappropriate images or videos

Inappropriate images or videos are any that are not directly relevant to the child's participation in the activities of BWFCC.

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.

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 is 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.

The inappropriate sharing of images or videos of children can have significant legal, ethical, and professional consequences. Individuals who engage in this misconduct will face disciplinary actions, including immediate termination, professional repercussions, suspension of individuals Working with Children Check (WWC), and even legal prosecution.

SAFETY AND PRIVACY

- Children's full names will not accompany photographs or images without explicit consent from parents/guardians.

- Identifying information (such as addresses or personal details) will not be disclosed in any image or video.
- Images will never be shared publicly on social media platforms or other public forums unless parents/guardians have provided specific consent for such use.
- All photos will be stored securely, and access should be restricted to authorised staff only.

STORAGE, ACCESS AND DESTRUCTION OF IMAGES

At BWFCC, the use, storage, and disposal of digital images and videos are governed by strict privacy and security protocols to safeguard children's personal information and uphold our legal and ethical obligations. All images and videos of children must be captured, accessed, and stored only on service-issued, password-protected devices. The use of personal or unapproved devices, platforms, or applications to download, transfer, or share media is strictly prohibited. To ensure the integrity and confidentiality of data:

- Staff and volunteers must not possess or use personal storage or file transfer devices (e.g. USB drives, SD cards, external hard drives, or personal cloud storage) while actively working with children.
- Digital images captured on service-issued devices are transferred monthly to a secure, password-protected central storage system (e.g. Microsoft Teams) with restricted access to authorised personnel only.
- Printed images or documentation are stored in locked, authorised-access areas (e.g. key-safe lockers) to maintain physical security.

To further protect privacy, BWFCC is committed to the timely and secure destruction of media that is no longer required:

- Digital files will be permanently deleted from devices and central systems once they are no longer needed for educational or administrative purposes.
- Printed photographs and documents will be shredded or securely destroyed by authorised (management) staff to prevent any unauthorised retrieval or misuse.
- For children who have ceased enrolment, all related images and documentation will be deleted or securely destroyed within 14 days of their final attendance, as managed by the Enrolments Officer.
- These procedures ensure that all digital and physical media are handled responsibly and respectfully, in alignment with privacy legislation, child protection requirements, and BWFCC's commitment to child safety.

USE OF EXTERNAL PHOTOGRAPHERS

- External photographers will provide evidence of a valid Working with Children Check or equivalent clearance before any images are taken.
- Families will be notified beforehand when the photograph sessions take place in our service.
- BWFCC currently partners with Vision Portraits (subject to change) to offer photography sessions for our families. As external photographers, Vision Portraits may seek consent directly from families regarding the use and potential publication of images taken during these sessions.
- BWFCC provides our own photography consent forms. These forms clearly explain how child(ren)'s images may be used, stored, and shared. They are designed to ensure families fully understand the purpose of the photography, and to give you the option to either give or decline consent.
- If any external photographer is hired by BWFCC to capture images or videos featuring children at the centre, families will be informed in advance, and a parent will need to provide written consent for their child's image to be included/published.

ELECTRONIC DEVICE USE:

- BWFCC staff and volunteers are not permitted to carry personal electronic devices that can take images or videos or personal storage media devices while children are at the centre. Staff must store personal storage media devices or personal storage media devices in their individual secure locker at the beginning of each shift. Staff are permitted to access their personal electronic devices during their breaks without children present and only in staff permitted areas (for example, when in the staff room or outside the centre).

Please note: the hallways are accessed by children therefore they are not staff permitted areas

- Only service-issued, password-protected devices are to be used to take images or videos of children while providing education and care, which includes but not limited to accessing or uploading documentation and communicating via approved platforms (e.g Xplor, Xplor playground, Outlook, Microsoft teams) (*see service devices section*)
- Personal electronic devices that can take images or videos, and personal storage and file transfer media (such as tablets, phones, digital cameras, smartwatches, META sunglasses, and other new and emerging technologies, where those technologies have image taking or video recording capability) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) are not to be in the possession of any person while providing education and care working directly with children, unless for authorised essential purposes such as emergencies, health and family needs.
- In cases of exemption, and with the employee's consent, centre directors should notify other staff about arrangements for the employee's personal electronic device. The reason for the exemption does not need to be shared. Centre staff with an exemption to carry their device must not use their personal device to take images or videos of children. E.g a staff member who has a family member with a serious illness.
- Written approval must be obtained before the staff or volunteer is permitted to be in possession of a personal electronic device when working with children. Such approval is given for the essential purpose only and the personal electronic device must not be used for any other purpose including taking images and videos of children.
- If a third-party professional attending a service and working directly with children (such as an allied health or inclusion professional) needs to use a device (for example, to undertake an assessment or take notes) they can use a device that is:
 - issued by their business or institution; and
 - used only for work purposes (and not a personal use).
 - while they are supervised

The restrictions on possession of personal devices do not apply to people who are not working directly with children.

Examples include:

- Parents and carers doing drop off and pick up (see visitors and families section for correct usage)
- Victorian Regulatory Authorised Officers, police and officers of other regulators, such as environmental health officers
- Third party contactors who are attending the service but not working directly with children or providing education or care (for example, maintenance contractors)

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 device is an essential means of communication for an educator or other staff member
- family necessity, e.g. a family member with a serious illness 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, e.g. bushfire evacuation text notification.
- to record an injury or if asked/instructed to take an image of a child by the Police or a Child Protection Agency

SERVICE ISSUED DEVICES

Only service issued devices are to be used to take images and videos of children. Service issued devices are those that are provided by BW FCC to staff for work purposes such as but not limited to supporting administration, communication and teaching learning programs.

All BW FCC's service issued devices will have:

- have an identification code
- are distinctly branded
- are easily identifiable from a distance.

All service-issued devices will be stored securely when not in use and a register will be maintained for the issuing and returning of these devices.

The following must be observed with respect to the use of service issued devices:

- Only service issued devices owned or operated by BW FCC may be used to connect to BW FCC's infrastructure or services
- Service issued devices must not be used by an employee's (staff) family or friends
- USB thumb drives or portable drives from an unknown or untrusted source are not to be connected to department equipment.

TAKING IMAGES AND VIDEO OF CHILDREN

Photos and videos of children will be used intentionally as part of implementing an educational program and assisting in documenting children's learning and development, which is our service's core purpose for taking images/videos of children.

BW FCC is committed to uphold these appropriate practices when taking images and videos of children:

- BW FCC staff can only take and access images and videos of children on service issued devices
- Taking images of children must primarily relate to children's learning, development and wellbeing and include taking active steps to ensure the safety, privacy and rights of individuals.
- Prior to taking images and videos, appropriate consents from parents must be obtained and respected. Due consideration should also be given to ascertaining children's assent to be photographed or filmed. This includes verbal or non-verbal assent such as smiling or nodding (to assent) or shaking head, turning away (showing dissent).

EXCURSION AND TRANSPORT

All digital technology use during excursions must:

- be conducted only with centre-issued devices
- remain consistent with consent agreements
- no personal devices are to be used during excursions to take photographs of children unless required for emergency purposes, communication and approved by the Nominated Supervisor.

VISITORS AND FAMILIES

Visitors including students, contractors, volunteers and families of BWFCC.

- All visitors, including families, students, contractors, and volunteers, are prohibited from using personal electronic devices (such as mobile phones, tablets, or cameras) to photograph or video any child other than their own.
- Parents and carers may capture images or videos of their own children only; however, photographing or recording any other children, even incidentally in group settings such as end-of-year celebrations, excursions, or other events, is strictly forbidden.
- All families and visitors will be made aware of this policy during their initial orientation and induction process.
- Clear signage reinforcing this policy will be prominently displayed throughout the Centre to ensure ongoing awareness and compliance.
- Families and visitors are prohibited from posting or sharing photographs or videos of children other than their own on any social media platforms or personal communication channels without the explicit consent of the other children's families.
- Prior to capturing images or videos of children other than their own during special occasions (e.g., Mother's Day celebrations, service-wide community events, welcome BBQs), visitors must obtain both verbal and written permission from the child's parent or legal guardian.
- Students on placement and volunteers must never take, use, or distribute photographs or videos of children without prior written consent from parents or guardians.
- When participation in photography or videography is required as part of their educational practicum or role, these images must be captured exclusively by authorised BWFCC staff using Centre-issued devices to maintain professional standards and compliance.
- Only BWFCC staff members are authorised to take photographs and videos of children for the purposes of documenting learning, communication with families, or Centre promotion. (with consent)
- In circumstances where students or educators on practicum need to document children as part of their study requirements, written parental consent must be secured in advance, and all images or videos must be taken by a staff member on an approved service device to protect child privacy and data security.

ONLINE ENVIRONMENT:

The Centre uses secure, approved platforms (e.g. Xplor, Xplor Playground, Microsoft Teams) for:

- family communications
- digital documentation and update of learning
- internal sharing of information

Staff are prohibited from:

- using unapproved platforms (e.g., personal emails, messaging apps e.g. whatsapp/facebook messenger/) to communicate with families, share documentation of children's learning
- sharing links, documents, or login credentials externally
- uploading identifiable information without consent

DIGITAL DEVICES USED BY CHILDREN

The use of digital technology within BWFCC's Early Childhood Education and Care (ECEC) programs is embedded within a broader play-based learning environment. Here, children's learning is dynamic, holistic, and child-centered, fostering active participation and exploration. In alignment with the Early Years Learning

Framework (EYLF), digital technologies and media enable preschool children to access global connections and resources, encouraging new ways of thinking, investigating, and problem-solving.

At BWFCC, digital devices are primarily utilised as teaching and learning tools by educators, rather than devices for passive consumption by children. Technologies are intentionally integrated into children's multimodal play experiences to enhance engagement and learning. Consistent with the Australian Government's physical activity guidelines, children aged 3 to 5 years should have no more than one hour of screen time per day, inclusive of usage at home.

BWFCC is committed to safeguarding the wellbeing and safety of all children in relation to digital technology use, which we adhere to the following:

- Children's use of digital devices is strictly supervised by educators at all times.
- Educators maintain direct line-of-sight to screens and continuously monitor children's online activities to ensure a safe and supportive learning environment.
- Children are not permitted unrestricted or unsupervised access to the internet or any online platforms under any circumstances at BWFCC.
- Educators are trained to promptly recognise and respond to any signs of distress or unsafe behaviour related to digital device use.
- To further promote safe use, risk assessments concerning digital technology are developed collaboratively with children. These assessments address online safety, appropriate device usage, and clear protocols for reporting unsafe or inappropriate content.

Where children access digital devices, their use must be:

- be part of the teaching and learning program
- appropriate to the age of the child
- strictly time limited
- modelled and supervised by an educator in shared spaces
- supportive of healthy posture to avoid strain when looking at devices or screen

Digital devices for children must:

- be service issued only
- have strong privacy settings enabled

Digital devices for children in ECEC services and programs must not:

- provide unrestricted and/ or unsupervised access to the internet
- enable any personal information, including images, to be uploaded
- be used as a strategy to manage children's energy, engagement or behaviour
- be used as a response to weather conditions

ARTIFICIAL INTELLIGENCE (AI) USE AND CONSIDERATION

At BWFCC, we are unwavering in our commitment to protecting the privacy, safety, and dignity of all children in our care. As part of this commitment, BWFCC strictly prohibits the use of Artificial Intelligence (AI) technologies that pose risks to children's identity, wellbeing, or digital safety.

AI technology, especially those involving facial recognition or image generation, presents serious risks in ECEC settings, including:

- Breaches of child privacy and consent
- Unauthorised distribution or manipulation of children's images
- Misuse of biometric data or metadata
- Loss of control over how children's identities are portrayed or used online

Given the inability of young children to provide informed consent and the irreversible nature of digital sharing, BWFCC strictly prohibits the use of AI technologies that could compromise child safety.

BWFCC does not permit the use of any AI systems or platforms that:

- Utilise facial recognition or facial detection technologies
- Generate, alter, or enhance images of children using AI or synthetic imagery (e.g., deepfakes or AI-generated faces)
- Collect, analyse, or store biometric data, including facial features or voice recordings
- Require the upload of children's personal information, photographs, or videos into third-party AI platforms (e.g., ChatGPT, DALL-E, Midjourney, FaceApp, etc.)

This restriction applies to both direct usage by staff and indirect usage through embedded AI features within apps or software.

These technologies are deemed inappropriate and high-risk within early childhood education settings due to:

- Inability to obtain informed consent from children
- Risks of data breaches, digital manipulation, and misuse of identity
- Misalignment with ethical, developmental, and safeguarding responsibilities in early learning environments

Only approved, educator-operated, service-issued devices and platforms are used to capture and share documentation of children's learning. All usage occurs with explicit parental consent and in secure, private environments that support educational and internal communication purposes only.

BWFCC will continue to monitor developments in AI technology to ensure our policies remain responsive, ethical, and aligned with best practice in child protection and digital safety.

All educators and staff must:

- Avoid using any AI-enabled tools (web-based or app-based) that request or process child-related content (images, videos, names, etc.)
- Ensure that no content involving children is uploaded into any AI platform for educational, creative, or administrative purposes
- Remain informed about potential AI features in applications they use and raise any concerns with the Centre Director
- Report any accidental exposure to AI platforms immediately for review and action

Third-party providers (e.g., photographers, allied health professionals, IT service contractors, or students on placement) must:

- Refrain from using AI tools during their engagement with the service
- Not upload or process any child images or personal data using AI applications

- Sign relevant data handling agreements, where required
- Only use BWFCC-approved devices and systems for documentation purposes

Families will be clearly informed that:

- BWFCC does not use AI for creating, editing, storing, or analysing children's images or data
- Their child's information will not be uploaded or processed through any AI platform
- Consent forms will clearly identify the platforms used and affirm the Centre's position on AI

Any breach of this AI Safety Addendum will be taken seriously and may result in:

- Disciplinary action (for staff, students, or volunteers)
- Termination of service agreements (for external providers)
- Notification to the Department of Education and Office of the Australian Information Commissioner (OAIC) or relevant authorities

ROLE RESPONSIBILITIES

The Approved Provider (Board of Governance) is responsible for:

The Bubup Womindjeka Family and Children's Centre Board of Governance is the Approved Provider and has ultimate responsibility for the management and control of the service. The Board delegates operational responsibility and day to day management of the service to the Nominated Supervisor and monitors the performance of the organisation, including responsibilities contained in this policy, through regular reporting and by ensuring appropriate resources are available to carry out the organisation's functions.

The Nominated Supervisor and Persons in Day-to-Day Charge is responsible for:

- Implementing the Safe use of digital technologies and online environments policy and procedures and ensure that any plans developed from risk assessments are in place for individual children and are carried out
- Ensuring staff understand how to actively supervise children while using digital technologies
- meeting staff to child ratios to ensure adequate supervision
- having ongoing communication with educators and staff about their responsibilities and any changes to policies, procedures, particularly as digital technologies evolve quickly.
- supporting educators and staff to uphold the service's culture of child safety and wellbeing, including when accessing digital technologies and online environments.
- supporting educators and staff to understand the National Model Code and manage the use of electronic and digital devices at service, including the service's expectations around the use of personal and service issued devices.
- ensuring that images are used respectfully and no personal electronic devices are used while working with children and in line with this policy.
- training staff in the appropriate use and handling of photos and images, including understanding the importance of consent, privacy and the strict prohibition of the use of personal electronic devices in the service
- ensuring staff induction will cover the importance and understanding of consent and privacy, as well as ensuring personal devices always stay out of the learning environment except for excursions.

Educators and staff responsibilities

- Ensuring that images are used respectfully, personal electronic devices are not used when working with children and in line with this policy and in accordance with the National Model Code.
- Adhere to this policy in line with our Code of Conduct Policy
- Staff will attend training in the appropriate use and handling of photos and images, including understanding the importance of consent and privacy

- Staff induction process will cover the importance and understanding of consent and privacy, and the prohibited use of personal electronic devices in the learning environment
- Ensuring personal devices always stay out of the learning environment except for excursions
- Follow the Information Communication Technology (ICT) policy.
- Ensuring that all images or videos captured are directly relevant to the educational program
- Ensuring that the use of BWFC issued electronic devices to document the education program does not impact the safe and effective supervision of children (see Supervision of children policy)
- Recognise and respond effectively to children when discussing the use of digital technologies and online environments, considering diverse needs and interests.
- Ensure children participate in decision-making in matters affecting them regarding the safe use of digital technologies and online environments at the service.

Parent/guardian engagement

- Families will be informed of this policy during orientation and updated regularly on the usage of photographs or images within the service
- Parents/guardians are encouraged to discuss any concerns they may have regarding the use of photos and images with educators
- Ensure personal devices are not being used to take photographs, videos (any content at all) of children (other than their own) in the learning environment

BREACHES OF POLICY

- Any breaches of this policy, including unauthorised sharing, misuse of photographs and the use of personal devices in the learning environment, will be treated seriously. A review will be conducted, and necessary disciplinary actions will be taken to prevent future breaches. Disciplinary action may include dismissal.

EVALUATION

The effectiveness of this policy will be evaluated regularly, every 3 months to ensure it is being followed and remains compliant with the current legislation, child protection guidelines, and best practices for privacy. This evaluation will involve:

- [conducting regular audits every term of how photographs and videos are taken, stored, and shared within the service to ensure compliance with consent protocols and privacy safeguards. Our admin team/enrolment officer will check consent forms of families enrolled in our service to ensure consent is given for any photography/videography of their child\(ren\). Communications will be sent out to all team members about children whose parents do not give consent.](#)
- ensuring images are stored in secure, centralised systems such as Microsoft Teams rather than Centre-issued Ipads, which reduces the chance of data breaches or loss.
- conduct spot-checks on device use in the learning environment
- review any device-related incidents or breaches
- conduct risk assessments for all digital technology use
- regularly seek feedback from everyone affected by the policy regarding its effectiveness
- ensure regular staff training and professional development opportunities to ensure that educators and staff are up to date with the policy and are consistently applying it.
- review process to update the policy as required, particularly considering any changes in legislation or guidelines surrounding child protection, privacy, or the use of digital media.
- notify parents/guardians at least **14 days** before making any changes to this policy or its procedures.

The review process will involve consultation with relevant stakeholders, including educators, families, and the board of Governance, to ensure the policy remains relevant, effective, and compliant with any new developments in child protection or privacy law.

Version History

Date	Version	Author/s	Details
August 2025	1.00	Director of Education	New Policy
April 2026	1.00	Executive Officer	Updated Regulatory Authority change (formerly Victorian Department of Education to VECRA Victorian Early Childhood Regulatory Authority)