Response to Child Safety Review

National Model Code & Guidelines

May 2024

#BestStartInLife

Contents

Introduction

The Australian Childcare Alliance (ACA) welcomes the opportunity to provide feedback on the proposed National Model Code and Guidelines for Early Childhood Education and Care (ECEC) services, specifically regarding the use of personal electronic devices and the taking of images or videos in ECEC settings.

The ACA advocates for and supports policy initiatives that prioritize the safety and well-being of children in ECEC settings, by implementing robust safeguards to prevent harm and create a safe, nurturing environment that fosters the healthy development of all children.

The consultation process around the first draft of the National Model Code and Guidelines provides an opportunity for early learning service providers to reflect on their own practices in terms of the use of photographs and videos in their day-to-day operations – this a powerful and productive outcome.

In reviewing the National Model Code, there are a range of considerations for services including:

- What is the purpose of taking images?
- Who owns devices used to take images/videos?
- How can we be sure who is taking those images/videos?
- How are those images/videos stored?
- What sort of platforms are they shared on?
- For what purpose are they shared?
- What sort of cyber security measures are in place?
- What sort of permissions exist from families?
- What happens in the case of events with families on site?

Importantly, the National Model Code takes a deeper look at the common practices of services including the use of personal electronic devices and beyond.

For example, while existing employment and operational policies in many long day care services prohibit staff from using personal devices such as mobile phones or tablets in the rooms, a common exception is the wearing of smart watches, which can have varying levels of technical capabilities depending on the specific model.

It is our intention to explore each of these considerations in more detail throughout this submission, to paint the picture of the practical implications for each. We also put forward a set of initial suggestions to enhance the model code by providing clearer guidance for service providers on the options available for managing the use of images and videos in ECEC settings.

Paul Mondo
President
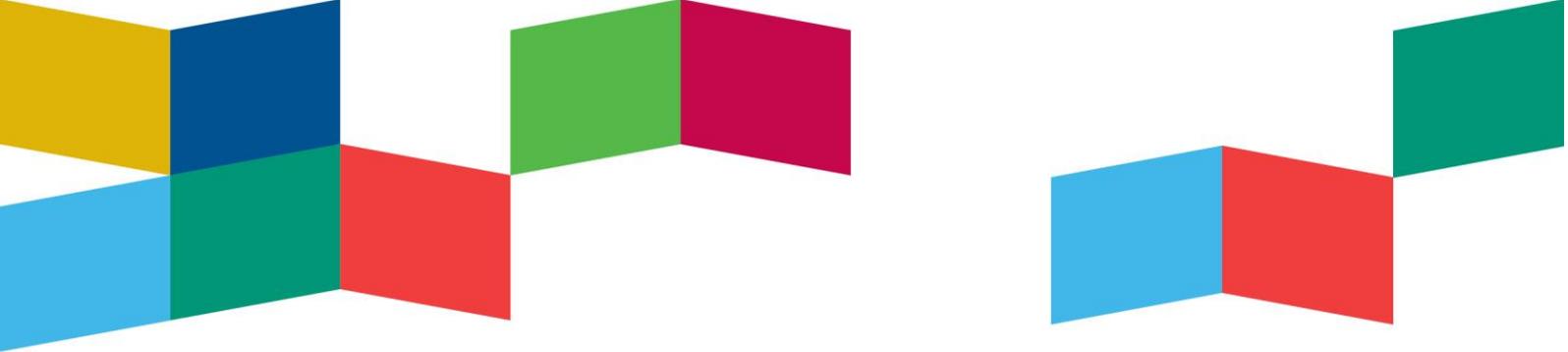
Taking images or videos in ECEC settings

What is the purpose of taking photos?

Early learning services may take images or videos in the context of operating their ECEC service for a variety of reasons.

These include:

- Observing developmental outcomes
- Assisting in the development of learning stories
- Creating displays within the service
- Updating parents on a how their child spent their day
- Connecting parents with the educational program
- Providing evidence for authorised officers regarding compliance and quality assessment
- For promotional and marketing purposes
- For events i.e. Mother's Day, end of year celebrations, etc
- For media purposes

Who owns the devices used?

Most ECEC services provide a range of devices to their educators and teachers for their day-to-day tasks.

These may include:

- Laptops
- Desktops
- Tablets
- Phones with no Sim card
- Digital cameras

These devices are generally made available for all staff in the room or for the whole team in the service to use as necessary. They may be used to take photographs of the educators and the children partaking in activities in the rooms or to finalise and record learning stories and developmental assessments in separate planning rooms or offices.

How can the service provider identify who is taking those images/videos?

In the context of existing practices, there is no reliable mechanism to clearly identify who was responsible for taking an image on a particular service owned device.
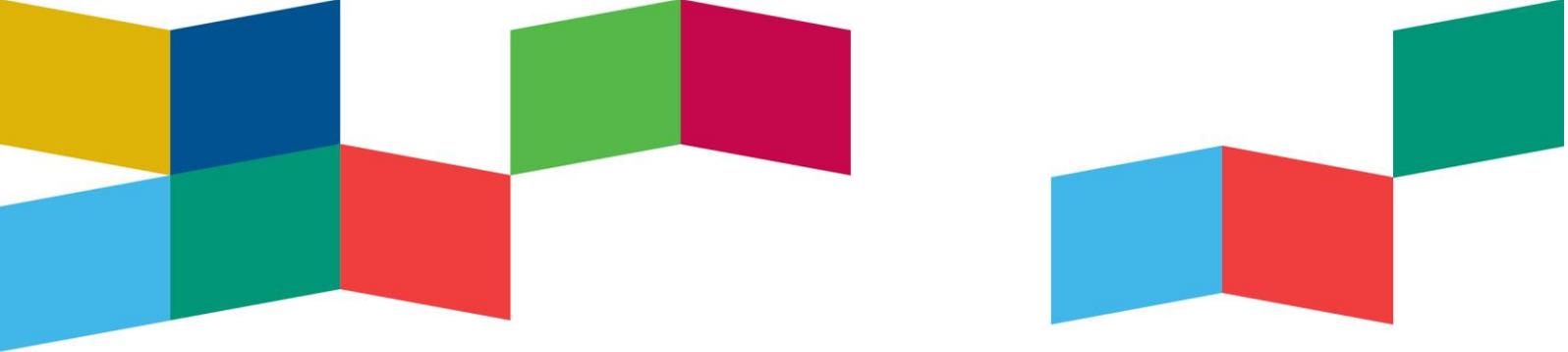
The standard practice in services does not include individual log-in procedures on each device in order for individual staff to access them. That is, for those services using devices with password protections in place, there is generally only **one password**, which is shared by numerous staff members. (Most smart phones and tablets are not designed to allow for more than one log-in & password.)

Additionally, in an ECEC service it is not standard practice for each educator/teacher to be given their own service-issued email address, as individual email addresses are generally not needed for all staff. On occasion there may be an email address provided for those staff working with a particular age grouping or in some cases one generic email address will be provided for use by all staff across the whole service. This adds another layer of complexity to being able to provide individual log-ins, regardless of whether or not the device will allow more than one log-in password.

Another complication around tracking the individual use of logins and passwords is that, unlike schools, it is common for educators to work across multiple rooms at a service. This means that individual staff members may have access to more than one email address, if these are provided on a room basis.

Trying to limit which educators are permitted to take photos can also be challenging in the context of covering staff absences, with replacement staff also needing access to the same passwords.

There have been suggestions that room leaders could be tasked with the responsibility of taking images. However, when implementing planned activities with the children, it is often the room leader who is directly involved leading the activity with the children, therefore requiring another educator to be in charge of taking the photos for later documentation purposes.
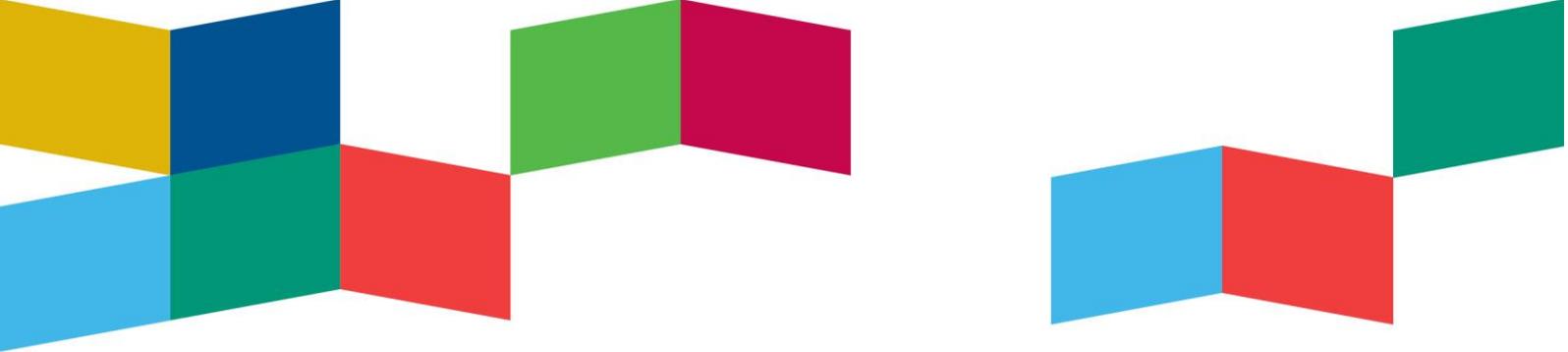
Storage & sharing of photos

How are images/videos taken in ECEC settings stored?

The mechanisms used to store images taken in ECEC settings vary from service to service.

ACA estimates the various methods used would include storage on:

- Service devices such as laptops and tablets
- Cloud solutions such as Onedrive, Dropbox or iCloud
- USB sticks and external hard drives

It is difficult to estimate how long images are generally stored for or how they are secured on these devices as this would also vary from service to service. In order to obtain accurate data on this topic, this would require detailed feedback from service providers, as part of a broader consultation, after they had been asked to reflect on this in more detail.

What sort of platforms are they shared on?

Whilst not the case in every service, a significant majority of ECEC services use a third party software provider such as Storypark, Owna or Kinderloop for the purposes of educational programming and sharing documentation for families. When utilised correctly these can be powerful tools to engage parents in their children's learning. These software platforms are a very useful and important tool, particularly when engaging with culturally and linguistically diverse families when there's a language barrier, which can make it hard to communicate quickly and easily.

In addition to these specific ECEC platforms, images can be shared on public social media platforms as well as private parent or educator groups on Facebook, Instagram, Whatsapp, etc.

For those services which don't use technology platforms for the purposed of documentation of children's activities, they are still likely to use Microsoft Word to collate documentation and store images on some of the earlier suggested devices/digital platforms.

For what purpose are they shared?

As previously outlined, the primary reasons for taking and storing images in early learning settings are:

- to engage families with their children's learning and daily activities; and
- to assist educators and teachers in assessing the children in their learning and development.

Service providers will also share images on social media to engage with the broader community. This can be an effective way to build awareness within the community, promote the service or for extended families to connect with service events.
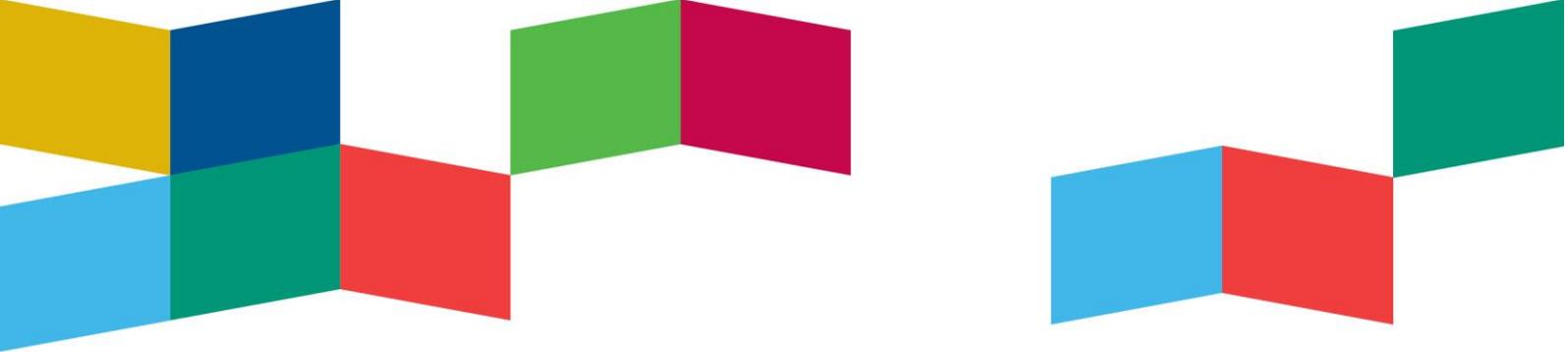
Security & Permissions

What sort of cyber security measures are in place?

Service issued laptops and desktops are likely to have a form of internet security software although it is likely that there is great inconsistency from service to service as to the type of security software used. It is highly unlikely that tablets run internet security software in any capacity as most providers would trust the relevant security provided by either Apples iOS or Google Android operating systems.

What sort of permissions exist from families?

ECEC services have long established policies for seeking permission from families before taking any images or videos of the children in their care. Generally these policies explain the purposes of taking photographs of the children already outlined on page 6 of this submission, with most families happy to give their permission in the interests of better engagement around their child's daily activities, their socialisation and their progress in learning and development.

The information around parental permissions to take photographs at the service is generally updated annually. This information is then shared across each room to ensure the educators have up-to-date permissions.

This practice is commonplace and appropriately respects the right for families to choose whether or not their child can be photographed during their attendance at the early learning service. Further consideration could be given to explore that the child grants permission of images or videos being taken to respect the rights and dignity of the child.

Photos taken by families at events

It is common practice for services to host a range of events at their services which invite parents, guardians and extended families including Mother's Day and Father's Day, end of year celebrations, graduations and art shows. These events are designed to value the service's broader community and enhance a better connection between the service and home environment.

At these events it is common for visitors to the service to bring their personal devices. Service providers remind families of relevant policies regarding the taking of images of children but often these families will still take photographs on the day. More often than not these images are only of their own children but as families usually have deep connections with other children and families at the service, this sometimes results in children other than their own being included in their photos.

In this context, it can be very difficult for educators to prevent families or visitors from taking photos in a busy and dynamic environment with lots of adults and children in a room. It is important to consider how these occurrences might be treated once the National Model Code is adopted at a service.

Specifically, does this mean that parents would not be allowed to bring their phones for photos on MothersDay as an example? Would services have to collect the devices of individuals before they enter a room with children?
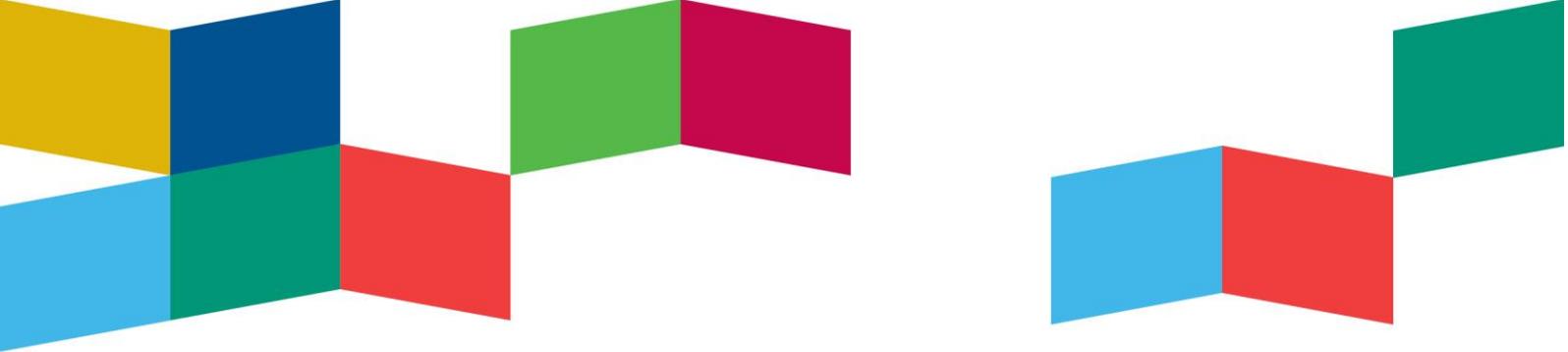
ACA position on the Model Code

Part 1

ACA supports this proposal, which is largely supported by existing practice in ECEC services.

Part 2

As per part 1, ACA supports this proposal which is again reinforced by existing operational policies in services.

It is uncommon that personal phones, cameras or tablets are used whilst directly working with children. However this is a far more complicated issue when it comes to smart watches, with many educators and teachers wearing them in the room on a day-to-day basis.

Whilst not all smart watches have cameras, the distinction between them is not easy to assess.

Furthermore, whilst some smart watches do not have cameras, they can be linked via Bluetooth to other devices such as phones or web cams to trigger the taking of images which of course creates risk.

ACA advised that doing an inspection to assess the digital capacity of each smart watch on a day-to-day basis is not a realistic outcome.

The situation is further complicated by the ongoing emergence of other digital devices on the consumer market such as smart glasses, which look like sunglasses but have integrated camera and audio functions, allowing for the surreptitious recording of conversations and taking of photographs.

ACA therefore recommends that the National Model Code includes prescriptive guidance on the use of smart watches by educators whilst directly working with children. We also recommend that the Code takes into account the constant evolution of new technologies and new devices, which may become more difficult to address as they become embedded in other products.

Part 3

ACA supports the process and list of essential purposes for the exemption of personal devices as defined in part 3.

ACA recommends further consideration for excursions to be included on this exemption list, given the logistics around these events. When undertaking risk assessments for an excursion it is important to consider a range of possibilities. The number of educators required to participate in some excursions means that there are simply not enough service operated mobile phones to match.

For example, a service takes eight educators on an excursion to the zoo. Once at the zoo those educators and children split into four groups, with two educators in each group. This would mean that the service would need to provide four service mobile phones or tablets with sim cards for the purpose of remaining in contact whilst on the excursion. This number of spare devices to be taken outside of the physical premises would not likely be available for most ECEC services, and therefore the personal devices of the educators would be relied upon.

Part 4

ACA strongly recommends that this section of the National Model Code should be explicitly defined with prescriptive guidelines, in order to remove all ambiguity in terms of its implementation for ECEC service
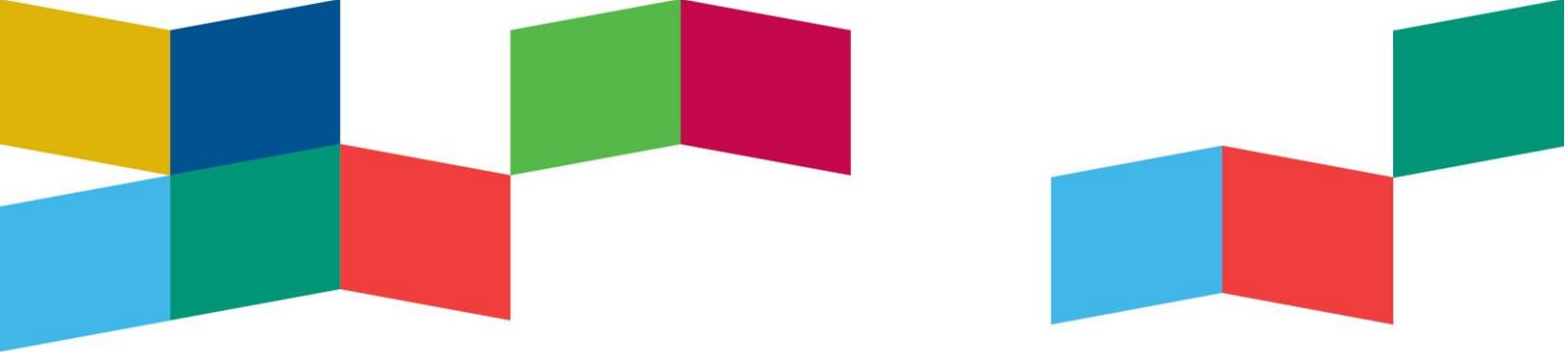
providers. As the early learning sector is made up of a diverse range of service provider types and scales, some of which have the benefit of large IT departments and some without, the guidance around IT requirements needs to presented in a way that is easy-to-understand for all service types.

In addition to the clarity of guidance, we also recommend the development of a defined approach and process, to ensure that this part of the code is not left open to interpretation, therefore risking accidental non-compliance with the National Model Code.
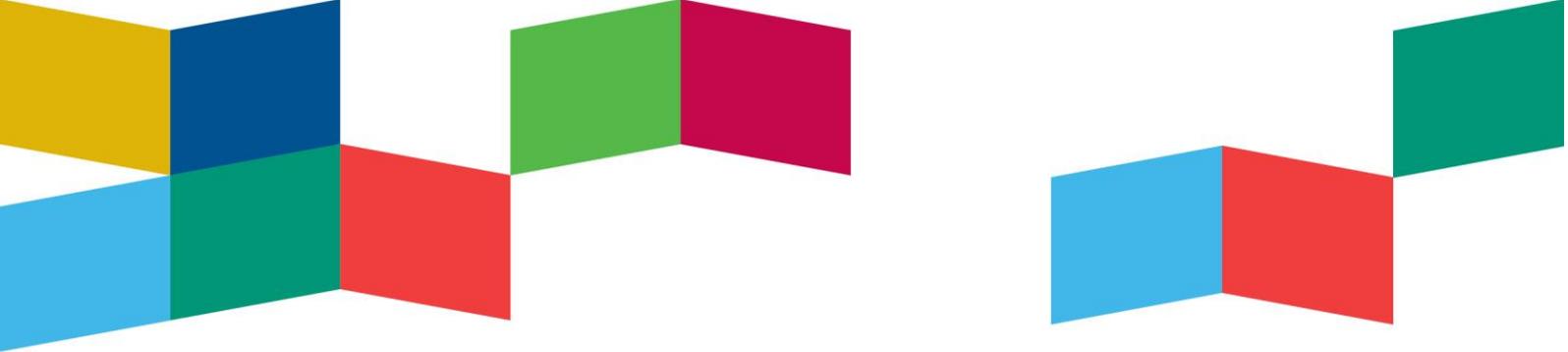
Broader risks and opportunities

There are a range of broader considerations that need some thought which are not specifically defined in the National Model Code.

Third party software

ACA recommends that an appropriate standard be established for these third party software providers to ensure that they cannot be a victim of a security breach.

For example: https://www.intertekinform.com/en-au/standards/as-nzs-iso-iec-27001-2023-115529_saig_as_as_3322596/

ACA has sought some information on this however it seems abundantly clear that the range of security protocols may not be best practice and vary significantly from one provider to another. These software packages that store images of children are sometimes registered third party software providers and the Government could mandate a specific protocol for these organisations to maintain the authority to be registered for CCS.

There are of course a range of software providers who do are not registered for CCS purposes and of course this could be difficult to enforce. One solution we propose is for these software providers to provide an annual certification that verifies the maintenance of the security protocol standard as defined by a relevant authority.

One other consideration is that each educator has an individual log in for these software platforms that they can access from any device, including at home. This provides a level of risk even if only service devices are used for the taking and uploading of images as these images can then be accessed via these platforms.

Service issued devices are generally connected to the internet which adds another risk as photos can be sent via email or other apps to personal accounts.

Service device arrangements

As discussed above it is impractical for each educator to have an individual log in for each service owned device. The impact is on all services however smaller services do not have the IT departments to implement these changes.

In some services senior management are paid phone allowances rather than being given a service issued phone. For the purposes of the model code, would these phones be deemed as personal devices? This as an important clarification that the model code needs to be clear about to ensure that services are correctly complying with the code.

ACA recommends that a clear ruling on whether a mobile phone being used by a service manager who is receiving a phone allowance is deemed a service issued device.

Parent expectations

One of the more challenging issue to unravel are the expectations of families with regards to the provision of images. There are many families who choose which service to send their child to on the basis of the number of photos provided by a parent app. This is unfortunately more common than not and more than a nuisance
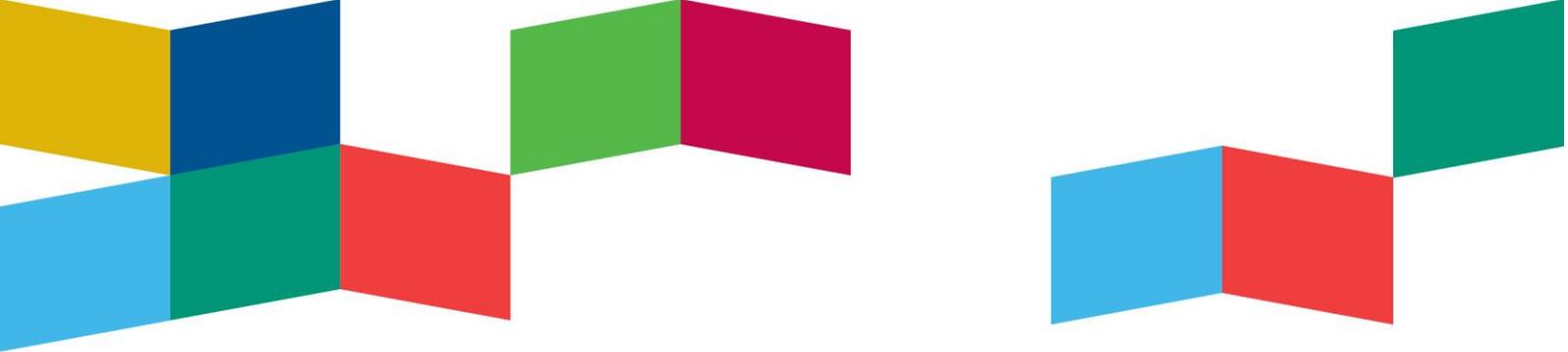
factor. Specifically this means that despite the best intentions of services, the decision to provide less photos can impact the viability of services.

ACA is supportive of measures to reduce the expectations of families with regards to taking photographs of their children but we would highly recommend the creation of some targeted guidance material by ACECQA to assist service providers with educating families on the new requirements under the code.

ACA recommends that ACECQA produces a range of communication materials that are ACECQA-branded for services to share with families to try to shift their expectations around the regular taking of photographs by educators and teachers.

Visitors to the service

At any one time there can often be a range of visitors to a service including tradesmen, incursion leaders and allied health professionals. Whilst it is clear that they are not allowed to take photos of children and that they are accompanied at all times, this is not fool proof.

For example; if the summer has a plumber attend the service and that plumber needs to take a photo of a part, it is relatively easy for additional images to be taken despite best efforts of the person supervising. At times this can be challenging in services who are experiencing staffing shortages.

ACA recommends guidance on whether visitors to services are allowed to hold personal phones on them whilst in spaces in and around children.

Evidence for Assessment and Ratings process or child protection

Images are often used as evidence in both a QIP and for Assessment and Rating purposes that include children. It can often be the case that this is an expectation from an authorised officer.

In addition ACA can cite examples of child protection officers requesting photos for the purpose of sharing with parents.

Service events

As discussed above service events are a valued part of service life. Naturally parent visitors carry personal devices on them whilst attending these events and it can be challenging for educators to monitor this closely at these intensively busy events.

ACA recommends clear guidance on what is realistically expected of services at service events with a high number of parent/family visitors.

Professional photographers

Services generally undertake a range of professional photography opportunities either for annual photos for parents to purchase or for other promotional opportunities. This extends to how these photographers store images. It is critically important that the model code deals with this in a clear way.

This extends to events when politicians visit services and invite media to attend.

ACA recommends that explicit guidance is provided on the expectations around professional photographers to guide service decision making.
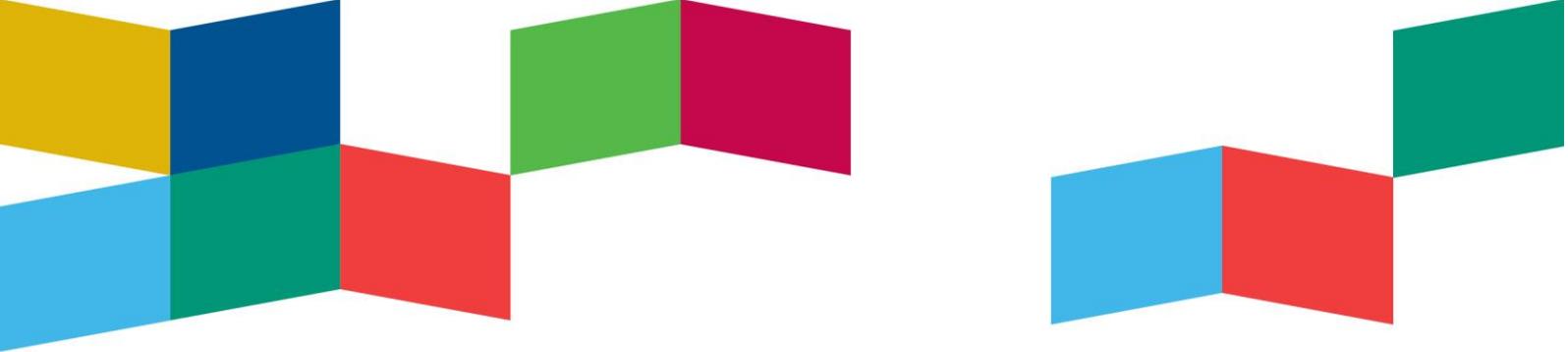
ACA Recommendations

ACA's comments above are intended to provide a practical understanding of the day-to-day practices of ECEC services and articulate the impact on current practice. This is not to suggest that changes should not be made, but rather to reinforce the need for appropriate education, communication and implementation time to ensure that services who adopt the model code are doing so in the full knowledge of the changes need to comply with it.

Whilst the model code will be via opt in to start with, once a service has opted in it is deemed as a service policy. There are therefore clear implications under the National Quality Standards should a services practice not align with its operational policies. History would suggest that regulators across the country may interpret these requirements differently as they so choose when it comes to assessment and rating or compliance visits.

Furthermore, what evidence will be sought to ensure a service has reflected on its practices to adapt the model code to its own unique context. Again, this may be interpreted in a variety of ways by authorised officers.

For the benefit of getting this right for the protection of children it is critical that a more specific information is provided in the guidelines to the model code to minimise a variety of interpretations.

ACA looks forward to further assisting and informing the model code and subsequent legislation as well as working constructively with ACECQA on its roll out in the months ahead.

RECOMMENDATIONS

In terms of developing a new National Model Code, ACA recommends:

- Broader sector-wide consultation is needed to ensure that the National Model Code is **fit for purpose** and effective rather than tokenistic and ambiguous.
- Ensuring that the code takes into account the practical limitations that apply to monitoring the use of digital devices within an early learning service – particularly for the smaller services.
- Ensuring that the recommendations within the code are **prescriptive** and **not** open to interpretation (i.e. crystal clear on which practices are /are not acceptable).
- Ensuring that the code is interpreted and implemented consistently across all state/territory jurisdictions.
- Ensuring that the code successfully addresses the possible use of evolving technologies (eg. smart phones, smart glasses and miniature spy cameras placed surreptitiously) plus ambiguous scenarios such as parents taking photos in the service.
- Ensuring that the code includes and enforces a legally approved national standard (via Standards Australia) for and accreditation of third-party software and other digital platforms that capture, store and/or publicly share images and videos of children.
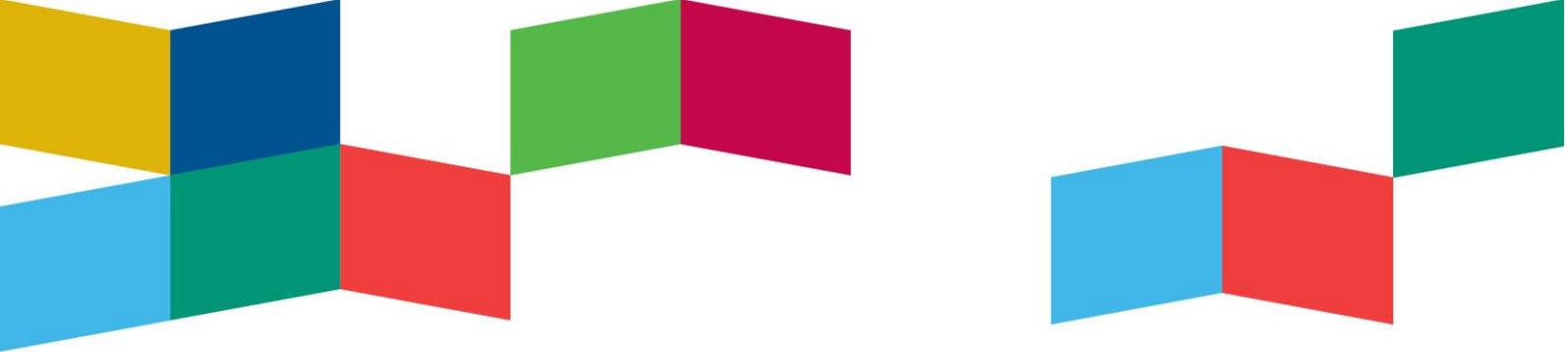
We recommend that the code should also outline how such third-party software and platforms will be required to manage (including receiving and deleting of) images and videos of children.

In terms of rolling out a new National Model Code (once finalised), ACA recommends:

- A comprehensive and thorough communications package to support early learning service providers in implementing the requirements of the National Model Code (i.e. ACA recommends guidelines that are far more comprehensive than the current guidelines provided).
  This guidance would need to include prescriptive guidance around the use of professional photographers for promotional purposes.
- A comprehensive communications campaign targeted at families, so that they understand the changes and assist with adjusting their expectations regarding the taking of photographs on the premises of their early learning service.
- A pilot program to be trialled across a broad range of early learning service types and sizes, to iron out any challenges that arise as the National Model Code is implemented.

Australian Childcare Alliance

Email: president@australianchildcarealliance.org.au

Website: www.childcarealliance.org.au

Phone: 0411 587 170

Facebook: www.facebook.com/childcarealliance

Australian Childcare Alliance
Queensland

Australian Childcare Alliance
New South Wales

Australian Childcare Alliance
South Australia

Australian Childcare Alliance
Victoria

Australian Childcare Alliance
Western Australia

Australian Childcare Alliance
Tasmania