Online Child Safety within Early Childhood Education

October 2025

aram
Advisory

Introduction

Within Early Childhood Education (ECE) there is significant focus on physical child safety for good reason. There are however interdependencies with Online Child Safety which are not well understood. The ECE online landscape is continuously evolving, presenting unprecedented challenges with the increasing digitisation of children's lives, the inclusion of 3rd party software providers and rapid proliferation of AI. Whilst data is limited on ECE specifically, the Education Sector as a whole has seen a significant rise in Cyber attacks accounting for almost 1 in 5 of critical sectors reported[1] with Australia reported as being the 4th most targeted country[2].

Approach

To evaluate the current state an investigation has been conducted which details major threats, emerging themes and best practice. A review of seven prominent Child Care Management System (CCMS) and Child Documentation software providers from publicly available information has been conducted and select Industry experts have been interviewed for their perspective.

The Importance of Early Childhood Development

The early years of a child's development is not well understood. Most of the focus from a pedagogical perspective is usually reserved for older children. However there is now more consensus that this is a particularly deterministic stage in a human being's life.

> **"In the first six years, children move through around 600 developmental milestones. By the age of three, we can already predict much of their life outcomes. That means that the early years give us a once-in-a-lifetime chance to unlock potential that lasts a lifetime."**
>
> **Himal Randeniya** , Mana CEO

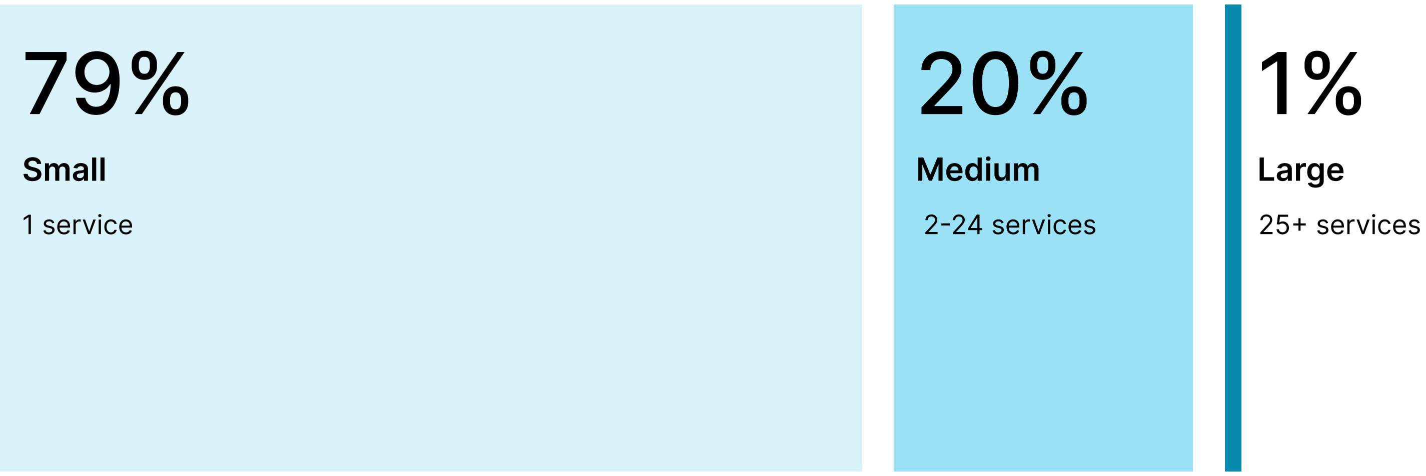
Proliferation of Threats and Emerging Themes

The online environment exposes children (typically 0-5 years old) within the ECE ecosystem to a growing array of indirect threats. The use of unlocked and personal devices, lack of robust cybersecurity controls coupled with less oversight of certain platforms make it challenging to control exposure.

The online environment exposes children (typically 0-5 years old) within the ECE ecosystem to a growing array of indirect threats. 79% of ECE Providers in Australia operate just one service and 20% operate 2-24 services[3]. The use of unlocked and personal devices, lack of robust cybersecurity controls coupled with less oversight of certain platforms make it challenging to control exposure.

Proportion of approved providers by size

7,194 Providers approved to operate under the National Quality Framework (NQF)



Smaller providers are more at risk as have less access to robust cybersecurity infrastructure and internal capability

Source: Adapted from ACEQA 2024 Q4 snapshot - https://www.acecqa.gov.au/sites/default/files/2025-03/NQF_SS_Q4-Feb25.pdf

Data Privacy - Sharing Sensitive Personal Data and Digital Footprint

Sensitive personal information (names, addresses, health information, developmental progress, photos and videos) are often stored on cloud-based CCMS or specific ECE documentation platforms which creates vulnerabilities. If these systems are not adequately secured, this data is susceptible to breaches, unauthorised access, or misuse.

Parental Involvement

In effect a child’s "digital footprint" within ECE is created by adults. Sharing photos and videos of young children online without their consent can have long-term privacy implications.

Vulnerability

Lack of robust cybersecurity infrastructure in ECE centers, insufficient staff training on data handling, and third-party software vendors which are not required to be secured with best practice (ISO 27001 / SOC 2) due diligence on privacy or security measures.

> **“Every photo, every piece of developmental data we upload about children online builds a digital profile of them. That profile can be used in ways that either enrich or seriously harm their future. That’s why securing it properly matters so much.”**
>
> **Himal Randeniya** , Mana CEO

Child Care Management Systems (CCMS) and Child Documentation Applications

At present CCMS software providers in Australia require approval under the Department of Education to participate in the Child Care Subsidy (CCS) system. However many ECE Providers utilise dedicated Child Documentation apps to track development and for parent-teacher communication (sharing photos, daily updates, and even confidential information) which do not require the same level of government oversight.

At present there is no requirement to have Cybersecurity best practice certification (ISO 27001 or SOC 2) for either a CCMS or Child Documentation software provider. Further 3rd Party APIs connect to CCMS to either pull or push information (e.g. compliance of an accident) and also have less oversight.

If these apps lack strong encryption, multi-factor authentication, or robust privacy settings, they can become a vector for data breaches. Unauthorised access to a parent or teacher's account could gain access to a child or expose sensitive video footage or images of children.

Vulnerability

Minimal security auditing of CCMS, Child Documentation and third-party apps leads to inconsistent application of security best practices and potential for app vulnerabilities.

Physical and Online Child Safety Interdependence

Smaller ECE Providers are particularly susceptible to cyberattacks. A successful attack could compromise sensitive child and staff data. With access to staff, child and parental data it is physical child safety that could be compromised. Further with access to unsecure video footage within ECE Centres sensitive child data can be used by malicious actors ongoing.

Physical child safety intervention unintentionally reducing online child safety

Physical Child Safety CCTV being installed for enhanced security may have a perverse unintended outcome if it is not a true closed circuit. If a cloud based solution from a 3rd party provider, sensitive content (e.g. Nappy changing or similar content) are at risk of being leaked.

Inadequate Online Child Safety controls creating physical safety risks

Gaining access to a CCMS or Child Documentation App with insufficient security, a malicious actor can use staff, parent and child data which could threaten physical safety.

Vulnerability

CCTV being implemented but content stored in Cloud with minimal oversight. Limited IT resources and cybersecurity expertise within smaller ECE providers, outdated software, weak passwords, and inadequate network security protocols. This applies to internal networks, staff devices, and any other shared technology used in the classroom.

Inappropriate Content Exposure and Unsupervised Contact

Young children, even with parental controls, can accidentally or inadvertently encounter content unsuitable for their developmental stage.

This can range from disturbing images or videos (violence, sexual content, gore) to age-inappropriate advertisements, or even content that promotes unhealthy behaviors. A single misclick or algorithm deviation can expose them to harmful content.

While direct interaction with strangers in online games or platforms might be less common for 0-5 year olds, it could still occur through communication features embedded in educational apps or games. These features might allow for chat functions or shared virtual spaces where adults posing as children or other malicious actors could attempt to initiate contact.

Vulnerability

Lack of supervision and a child's inability to differentiate between "good" and "bad" content, that might lead them to click on enticing but harmful links or pop-ups.

> **“I think that parents don't understand how important it is for parental locks and constant supervision. If they're taking their device with them out of the room children could easily be exposed to unsuitable content.”**
>
> **Nesha Hutchinson** ,
> VP Australia Childcare Alliance

AI Opportunity & Online Safety

AI is being implemented within ECE with the intention to improve Child Development outcomes and reduce operational burdens. Targeted Apps and Connected Toys are now commonly used within these contexts.

> “We believe deeply in the potential of AI to help solve a very broad range of societal and business challenges. It is a transformative technology and we need to pursue it responsibly, with the right guardrails in place.”
>
> **Paul Migliorini**, VP ANZ Google Cloud

Safety & Trust

Beyond traditional online safety concerns, the emergence of Artificial Intelligence (AI) introduces new complexities.

AI-powered Apps can be used for content recommendation, targeted advertising and even the creation of realistic but deceptive content (deepfakes), all of which pose risks to children if not supervised responsibly. The ethical implications of AI in data collection and algorithmic decision-making, particularly concerning minors, require careful consideration.

From a parent's perspective, there is a risk of trusting incorrect information generated by AI, such as false learning stories, which can betray trust and devalue the child, parent or teacher experience. There is also potential for real child engagement with educators to reduce as Providers increasingly rely on AI.

> **“We’re already seeing the impact of children growing up as digital natives: rising introversion, lower resilience. Without the right guardrails, AI could amplify these challenges for today’s youngest generation.”**
>
> **Himal Randeniya ,** Mana CEO

Finally as IT Management further leverages AI for standard or routine tasks, it leaves them vulnerable during outages or when systems go offline. Over-reliance on third-party vendors for AI-powered security technologies, particularly for smaller organisations that may not understand how these complex systems truly work or what to do if they fail.

> **"There's no ring fencing or guardrails around the use of data on Chat GPT or other platforms. We know Educators are actively using these platforms."**
>
> **Nesha Hutchinson ,**
> VP Australia Childcare Alliance

> **“The other Risk of using AI Development tools is staff not engaging with children.”**
>
> **Nesha Hutchinson ,**
> VP Australia Childcare Alliance

> **“The less apparent risk associated with AI lies in its potential to diminish healthy human interaction, and as its influence grows, could significantly impede children's ability to integrate effectively into society."**
>
> **Elrich Engel ,**
> Google Senior Security Advisor

> “The less apparent risk associated with AI lies in its potential to diminish healthy human interaction, and as its influence grows, could significantly impede children's ability to integrate effectively into society."

Elrich Engel, Google Senior Security Advisor

> “The industry is increasingly reliant on vendors which use AI but don't know how it works. If that vendor goes offline it creates a big problem for larger organisations however what do smaller organisations do when they're so reliant on this technology?”

Sean O'Donoghue, CIO BestStart

Best Practices & Certification

To mitigate online risks and ensure a secure environment for children, adherence to recognised best practices is crucial for CCMS and ECE Software providers.

Best Practices & Certification

There are internationally recognised frameworks and standards which provide a structured approach to data protection, information security and AI management.

SOC 2 (System and organisation control 2)

An independent report on controls relevant to security, availability, processing integrity, confidentiality, or privacy. It assesses how well a service provider handles sensitive data.

ISO 27001 - Information security management systems (ISMS)

A globally recognised standard that provides a framework for organisations to manage and protect their information assets.

ISO 42001 - Artificial intelligence management system (AIMS)

An emerging standard specifically designed to provide guidance on managing AI systems responsibly, addressing concerns like transparency, fairness, and accountability.

> **“First and foremost, develop products and technologies that ensure safety and security are baked into the core design, not an afterthought. Consider robust privacy settings, content filtering, and comprehensive monitoring capabilities.”**
>
> **Elrich Engel**, Google Senior Security Advisor

Child Documentation and CCMS Online Safety Review

A desktop review of select ECE Child Documentation and CCMS providers was conducted. Four dimensions across Cybersecurity, Transparency, Consent and AI Risk have been considered.

Child Documentation and CCMS Online Safety Review

Summary Findings

All Providers claim reasonable steps in terms of Cybersecurity however limited 3rd party auditing and verification. Review insights:

1

Child Documentation players have less regulatory oversight than CCMS players who require approval to participate in the CCS system.

2

There are traditional CCMS or Child Documentation players which are now providing both offerings (e.g. OWNA, xplor).

3

Mana was the only provider reviewed which has independent SOC 2 and ISO certifications however most claim to use best practice controls.

4

Parental Consent is usually obtained as a one off at a point in time or a default whilst using the service.

5

How Users can request data to be deleted is not always clear depending on the provider.

6

Many providers are yet to implement an AI Management System however there is more focus from select providers.

1 Cybersecurity

1a Data Collection & Usage	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Clearly Identify Data types Collected	3rd party verified	Claimed^	Claimed	Claimed	Claimed	Claimed	Claimed
Explains any third-party access to Children's data	3rd party verified	Claimed^	Claimed	Claimed	Claimed	Claimed	Claimed
Explains how sensitive data (addresses, photos, identity details, health, disabilities) is used & encrypted	3rd party verified	Claimed^	Claimed	Encryption not disclosed	Claimed	Claimed	Encryption not disclosed

1b Data Retention, Security, and Breach Management	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Publicly specifies how long personal data is retained	Claimed	Claimed*	Claimed	Claimed	Claimed	Claimed	Claimed
Describes encryption in transit and test & lists hosting providers (e.g. AWS)	3rd party verified	Claimed^ (AWS hosted in Australia)	Claimed	Not disclosed	Claimed	Claimed (AWS hosted in Australia)	Claimed (AWS hosted in Australia)
Explains how access to data is controlled internally	3rd party verified	Claimed^	Claimed	Claimed	Claimed	Claimed	Claimed

1c Intrusion Detection	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Intrusion Detection: Measures in place to detect unauthorized access or cyberattacks	3rd party verified	Claimed^	Claimed	Claimed	Claimed	Claimed	Claimed

1d Security / Privacy Policy	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Privacy policy is easy to find, readable and updated within last 12 months	Yes (Last update 1.8.24)	Yes	Yes (Unclear when last updated)	Yes	Last updated May 2023	Last updated May 2023	Yes (Last update 1.8.24)

Low confidence ⟷ **High confidence**

Not disclosed	Claimed	3rd party verified

*No timeframe exists and child data is retained indefinitely unless parent opts to delete their child's profile

^Storypark confirmed working towards ISO 27001 / 42001 and SOC 2 Certifications

Note: All providers were contacted for confirmation of above details however at time of publishing responses from Owna, XAP and Kidsoft were not obtained

2. Transparency / Accountability / Ethics

2a Ethics / Transparency	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Ethics Policy or Terms of Service is in plain language terms, including clauses on user rights and use of data Advanced - Trust Centre and 3rd Party Verified	Yes (Trust Centre & 3rd Party Verified)	Yes	Yes	Yes	Yes	Yes (Trust Centre)	Yes (Safeguarding Policy)

3. Parental Consent and Data Deletion

3a Parental Consent	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Explains how verifiable parental/guardian consent is obtained and renewed	Not disclosed	Yes (Consent obtained by use)	Yes	Yes (Point in time Consent)	Yes (Point in time Consent)	Yes (Consent obtained by use)	Yes (Consent obtained by use)

3b Data Deletion	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Users can request deletion of personal data and process clearly explained including timeframes	Yes	Yes	Yes	Yes	Yes (Request in writing)	Yes (Request in writing)	Not disclosed

4. Mitigating AI Risk

4a AI Risk	Mana	Storypark	Educa	xplor	OWNA	Xap	Kidsoft
Have an AI Management System in place to monitor and protect use of child data	3rd party verified	No but AI Fact Sheet exits^	Claimed	Not disclosed	Not disclosed	Claimed	Not disclosed

Low confidence ⟷ **High confidence**

Not disclosed	Claimed	3rd party verified

^Storypark confirmed working towards ISO 27001 / 42001 and SOC 2 Certifications

Note: All providers were contacted for confirmation of above details however at time of publishing responses from Owna, XAP and Kidsoft were not obtained

> “I highly recommend ECE Centres verify the security standards that these technology providers or manufacturers are publicly compliant to, (e.g. ISO standards), along with their stated position on the adoption of industry best practice cybersecurity frameworks."
>
> **Elrich Engel ,** Google Senior Security Advisor

> “Audited security programs are still the exception rather than the norm in our sector. That’s not because they’re out of reach or too costly. Programs like these are the norm in other sectors. It’s because they haven’t been prioritised. By taking this step, we can transform online safety from a weak point into a strength we’re proud of as a sector.”
>
> **Himal Randeniya ,** Mana CEO

Recommendations

Online Child Safety requires cooperation between government, industry, and non-profit organisations to address emerging threats. There are some nearer term immediate steps which ECE Providers and Software Providers can take to better protect children. Further over the mid to longer term other stakeholders including larger Technology and Connectivity Providers along with Government can make meaningful systemic change.

ECE Providers

Ensure a base level of Cybersecurity protocols utilising guidelines from Australian Childcare Alliance and Australian Children's Education and Care Quality Authority (ACECQA)[4]. These include:

- Implement controls on devices and content sharing.
- Discuss safe and appropriate technology practices within Centres.
- Review current suppliers Cybersecurity approach.
- Provide locked-down, center-issued devices to prevent staff from using personal devices and accessing unauthorised apps.
- Review the use of AI-powered educational tools and connected toys in Centres.

Parents/ Guardians

Parents may not understand that they have significant influence for the online safety of their child. Tangible steps include:

- Advocate for and discuss safe and appropriate technology practices with your Centre and at home.
- Obtain opt-in permission for retention of your child's data, particularly photos and videos.
- Rally for a common standard of security that all software providers must adhere to.

> **"Online child safety, much like physical child safety, is a team sport. In the ECE context this requires collaboration between Providers, Parents, Policy Makers and Technology Suppliers"**
>
> **David Gnanapragasam ,** Director Aram Advisory

Policy Makers

Building on the recent Victorian Government Rapid Child Safety Review[5] Policy Makers can develop clear guidelines and accountability frameworks for ECE providers and Software providers. These can include:

- Implementing regulation for Child Documentation software providers extending on CCMS providers.
- Increase best practice safety standard requirements for Child Documentation and CCMS players handling sensitive information such as CCS or Child Development data.
- Ensure only true closed circuit CCTV to be used and accessed by on site security or Police.
- Establish guidelines around where children's data is stored, especially photos and videos.

Child Documentation & CCMS Providers

It is recommended that CCMS and Child Documentation players claiming best practice cybersecurity and AI management frameworks take reasonable steps for 3rd party verification and certification.

- Develop content and materials to help ECE providers and other ecosystem partners similar to explor's Cyberscurity guide[6]
- Roll out internal training and processes to enhance online child safety (e.g. password control in training and other environments) and appoint an Online Child Safety champion within the organisation to drive focus and initiatives.
- Collaborate with peers and other industry players to ensure the most safe online environment for children.

Technology Security Vendors / Interest Groups

There is potential to develop multi-tenanted security solutions that cluster services at a discounted rate for groups of Centres (e.g. firewalled ring-fenced approach with geo-blocking) which can be beneficial for smaller providers. It may be that private institutions, rather than the government may need to drive these collaborative security initiatives.

Technology Mobile Device Management (MDM) Partners with Policy Makers

Major Technology providers could provide a closed-off digital environment for third-party parent engagement applications that integrate with SMS systems. Platforms could implement screenshot blocking, alert mechanisms for unauthorised data sharing, and image recognition technology to prevent inappropriate content from being stored or circulated.

Larger Technology or Telecommunication providers can incorporate default security features either at the network level or on each device, such as image and video blocking at the camera roll. A solution is needed with oversight from the Government for an economic model with the right incentives.

“Policy updates and subsidies may be crucial to ensure that all providers, regardless of size, can implement top-tier security for children's safety, avoiding a scenario where cheaper less effective solutions are adopted just to tick a box”

Sean O'Donoghue, CIO BestStart

Conclusion

The rapid digitisation of the Early Childhood Education (ECE) sector, while offering significant benefits, has created a complex and evolving landscape of online risks.

The analysis reveals several vulnerabilities

The rapid digitisation of the Early Childhood Education (ECE) sector, while offering significant benefits, has created a complex and evolving landscape of online risks.

This report highlights the critical interdependency between online and physical child safety, demonstrating how vulnerabilities in one area can directly compromise the other. The proliferation of third-party software, including Child Care Management Systems (CCMS) and unregulated Child Documentation apps, coupled with the increasing use of AI, exposes young children to a growing array of indirect threats.

Key vulnerabilities

1

The lack of robust cybersecurity infrastructure in smaller ECE centers and insufficient staff training

2

A regulatory environment that does not mandate internationally recognised security standards like SOC 2 or ISO 27001 for all relevant software providers

3

Parental consent for data use is often a one-time process, with unclear mechanisms for data deletion

4

AI technologies introduce new complexities related to data privacy, content generation, and potential over-reliance

Conclusion

To mitigate these risks, a multi-faceted approach is required. As a starting point ECE centers must implement basic cybersecurity protocols to manage devices. Parents and guardians can advocate for better security standards and clear data policies. Critically, regulatory bodies and technology providers must act to:

1

Improve oversight of CCMS and Child Documentation apps, ensuring best-practice security standards for all providers handling sensitive child data

2

Provide a framework and incentive structure for a multi-tenanted model for Security Specialist organisations to service the smaller ECE Providers

3

Develop collaborative models with major technology and telecommunications companies to embed security features by default

By taking these steps, the ECE sector can build a more secure digital environment that protects the well-being of those most vulnerable.

Appendix

Child Documentation and CCMS Review Sources

Mana

https://trust.makemana.com/

https://www.makemana.com/privacy-policy

https://www.xplortechnologies.com/privacy-notice/

xplor

https://www.xplortechnologies.com/privacy-notice/

https://www.xplortechnologies.com/wp-content/uploads/sites/13/2024/05/Master-Terms-of-Service-SAAS-Australia-Version-1-2.pdf

https://www.ourxplor.com/guides/cyber-security-for-ece/

Storypark

https://main.storypark.com/privacy-policy

https://help.storypark.com/en/articles/10114616-storypark-artificial-intelligence-ai-fact-sheet

https://lp.storypark.com/sa/ai-at-storypark#:~:text=Guided%20by%20commitments-,Our%20Responsible%20AI%20Commitments,-Since%20we%20started

https://21365280.fs1.hubspotusercontent-na1.net/hubfs/21365280/Product%20Resources/Implementing_AI_in_ECE_guide.pdf

OWNA

https://owna.com.au/security-policy/

https://owna.com.au/terms-and-conditions

Educa

https://www.geteduca.com/privacy-policy/

https://www.geteduca.com/terms-and-conditions/

Kidsoft

https://kidsoft.com.au/security/

https://kidsoft.com.au/privacy-policy/

https://kidsoft.com.au/terms-and-conditions/

XAP

https://xap.net.au/trust-security/

https://xap.net.au/privacy-policy/

https://xap.net.au/xap-terms/

Footnotes

[1] ASIC Annual Cyber Threat Report 2023-2024
https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024#:~:text=The%203%20most%20common%20cyber%20security%20incident,*%20compromised%20asset%2C%20network%20or%20infrastructure%20(12%25).

[2] Australian Cybersecurity Magazine 2021 Report
https://australiancybersecuritymagazine.com.au/education-sector-sees-29-increase-in-attacks-against-organisations-globally/

[3] ACECQA Q4 2024 Report
https://www.acecqa.gov.au/sites/default/files/2025-03/NQF_SS_Q4-Feb25.pdf

[4] ACECQA Safe Use of Digital Technologies and Online Environments
https://www.acecqa.gov.au/sites/default/files/2025-07/PolicyGuidelines_SafeUseOfDigitalTechOnline_final.pdf

[5] Victorian Government Rapid Child Safety Review
https://www.vic.gov.au/rapid-child-safety-review

[6] Xplor Cyber Security for ECE guide
https://www.ourxplor.com/guides/cyber-security-for-ece/

aram
Advisory

Aram Advisory's focus is on finding fundamentally better ways to do things. Aram Advisory work with clients to develop unique approaches, challenging them to think big to achieve the best outcomes for all stakeholders and the world at large.

David Gnanapragasam

Director and Principal Consultant

Aram Advisory is led by David Gnanapragasam who has over 15 years management consulting, strategy and execution experience. He is passionate about Online Child Safety and healthy interaction with technology. David has worked with C-suite and seniors leaders of major organisations in Australia to mitigate their Cybersecurity risk. Recently he has also led complex programs in the Education sector to achieve beneficial outcomes for Educators, parents and children.

Email

david@aramadvisory.com.au

Phone

0415 304 375

Acknowledgements

This report was compiled with expert perspectives to share real world experience and practical solutions. Aram Advisory expresses appreciation to Nesha Hutchinson (Australian Childcare Alliance), Sean O'Donoghue (BestStart), Himal Randeniya (Mana), Elrich Engel and Paul Migliorini (Google ANZ) for their contributions.