

## POLICY – CYBER SAFETY

|    |  |          |
|----|--|----------|
| 1. | <b>National Quality Standards</b> .....                                  | <b>1</b> |
| 2. | <b>Purpose</b> .....   | <b>1</b> |
| 3. | <b>Scope</b> .....   | <b>1</b> |
| 4. | <b>Background</b> .....  | <b>2</b> |
| 5. | <b>Implementation</b> .....  | <b>2</b> |
| 6. | <b>Feedback</b> .....  | <b>4</b> |
| 7. | <b>Approval and Review Details</b> .....                                 | <b>4</b> |
|    | <b>Appendix 1 Education and Care Services National Regulations</b> ..... | <b>5</b> |
|    | <b>Appendix 2 Resources</b> .....  | <b>5</b> |
|    | <b>Appendix 3 Source</b> .....   | <b>5</b> |

### 1. National Quality Standards

| Quality Area 2: Children’s Health and Safety |                                   |   |
|--|-----------------------------------|---|
| Area   | Concept                           | Descriptor  |
| 2.2  | Safety                            | Each child is protected   |
| 2.2.1  | Supervision                       | At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.                                 |
| 2.2.2  | Incident and emergency management | Plans to effectively manage incidents and emergencies are developed in consultation with relevant authorities, practiced and implemented.         |
| 2.2.3  | Child Protection                  | Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect. |

See appendix 1 for Education and Care Services National Regulations.

### 2. Purpose

- 2.1 To create and maintain a cyber safe culture that works in conjunction with Baringa’s philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, educators and families. *‘All children have the right to experience quality education and care in an environment that provides for their physical and psychological wellbeing and provides support for each child’s growing competence, confidence and independence.’* Quality Area 2, ACECQA.

### 3. Scope

- 3.1 This policy applies to children, families, staff, management, and visitors of Baringa.

## 4. Background

- 4.1 Cyber Safety encompasses the protection of users of technologies that access the Internet, and is relevant to devices including computers, iPads and tablet computers, mobile and smart phones and any other wireless technology (including personal wearable devices - smart watches). With increasingly sophisticated and affordable communication technologies, there is a candid need for children and young people to be informed of both the benefits and risks of using such technologies. More importantly, safeguards should be in place to protect young children from accidentally stumbling upon or being exposed to unsuitable material or content.

Baringa has demanding cyber safety practices and education programs in place, which are inclusive of appropriate use agreements for Educators and families. Our educational software program provides families with up to date information about their child's development in way of regular reports, observations, photos, portfolios and email communications.

The cyber safety agreement includes information about the software program, Baringa's obligations and responsibilities, and the nature of possible risks associated with internet use, including privacy and bullying breaches. Upon signing Baringa's service agreement, families and educators will have access to the educational software program.

## 5. Implementation

- 5.1 Baringa uses an online secure platform which allows children, educators and families to share observations, photos, videos, daily reports, and portfolios. Families are able to view their child/children's learning and development and contribute general comments relating to their child or comment on an observation or daily report. The online platform includes the curriculum, framework and Baringa philosophies and has been customised to align with our practice. It provides child-centred design to allow educators to effectively plan with families, gather evidence and analyse and report on each child's learning journey, unique interests and family involvement.
- 5.2 Educators are alerted when a family member has added a comment. Likewise, families are notified when a relevant educator has posted a photo/comment about their child.
- 5.3 Access to a child's information and development is only granted to a child's primary guardians who may provide access to others if they wish. No personal information is shared with any third party.
- 5.4 Confidentiality and privacy:
- The principles of confidentiality and privacy extend to accessing or viewing and disclosing information about personnel, children and/or their families, which is stored on Baringa's network or any device.
  - Privacy laws are such that educators or other employees should seek advice from Centre Management regarding matters such as the collection and/or display/publication of images (such as personal images of children or adults), as well as text (such as children's personal writing)
  - A permission to publish form must be signed by parents to ensure children's privacy, safety and copyright associated with the online publication of children's personal details or work.
  - All material submitted for publication on Baringa's Internet/Intranet site should be appropriate to Baringa's learning environment.
  - Material can be posted only by those given the authority to do so by Centre Management.
  - Centre Management should be consulted regarding links to appropriate websites being placed on Baringa's Internet/Intranet (or browser homepages) to provide quick access to sites.
- 5.5 Centre Management will ensure:
1. All staff, families and visitors are aware of Baringa's Code of Conduct and Confidentiality and Privacy Policies.
  2. Baringa ensures that anti-virus and internet security systems including firewalls can block access to unsuitable web sites, newsgroups and chat rooms. However, none of these tools are fool proof; they cannot be a substitute for active adult supervision and involvement in a child's use of the internet.

3. Backups of important and confidential data is made regularly (monthly is recommended).
4. Backups are stored securely either offline, or online (using a cloud-based service).
5. Software and devices are updated regularly to avoid any breach of confidential information.

5.6 Nominated Supervisor/Responsible Person/Educators will:

1. Ensure to use appropriate netiquette and stay safe online by adhering to Baringa's policies and procedures.
2. Keep passwords confidential and not share with anyone.
3. Log out of sites to ensure security of information
4. Never request a family member's password or personal details via email, text, or Messenger.
5. Report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes you feel uncomfortable (See 'Resources' section for where to report).
6. Permission for children to use computers is obtained by parents as part of the enrolment procedure.
7. Ensure that children are never left unattended whilst a computer or mobile device is connected to the internet.
8. Personal mobile phones are not used to take photographs, video or audio recordings of children at Baringa.
9. Only use educational software programs and apps that have been thoroughly examined for appropriate content prior to allowing their use by children.
10. Provide parents and families with information about the apps or software programs accessed by children at Baringa.
11. Ensure that appropriate websites are sourced for use with children **prior** to searching in the presence of children.
12. Use a search engine such as 'Kiddle' rather than Google to search for images or information with children (See 'Resources' section).
13. Notify the Office of the Australian Information Commissioner (OAIC) by using the online [Notifiable Data Breach Form](#) in the event of a possible data breach. This could include:
  - A device containing personal information about children and/or families is lost or stolen (parent names and phone numbers; dates of birth, allergies, parent phone numbers).
  - 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 (portfolios, child developmental report)
  - This applies to any possible breach within Baringa or if the device is left behind whilst on an excursion

5.7 Families will:

1. When sharing anything using technologies such as computers, mobile devices, email, or any device that connects to the internet it is important you and everyone else invited to your account understands about netiquette and staying safe online and ensures privacy laws are adhered to.
2. When it comes to your own children, it is your choice what you share outside of Baringa. Remember though that young children cannot make their own decisions about what gets published online so you have a responsibility to ensure that whatever is shared is in your children's best interests.
3. Be mindful of what you publish on social media about your child as this may form part of their lasting digital footprint.

4. Install Family Friendly Filters to limit access to certain types of content on devices such as mobile phones and computers.
5. Install parental controls on streaming services to ensure children are not able to access inappropriate material.
6. Consider developing a *Family Tech Agreement* to establish rules about use of devices at home.
7. Sometimes other children in Baringa may feature in the same photos, videos, and/or observations as your children. In these cases, never duplicate or upload them to the internet/social networking sites or share them with anyone other than family members without those children's parents' permission.
8. Access further information about eSafety to help protect your children and be cyber safe.

**6. Feedback**

Families and staff may provide feedback about this document by emailing [admin@baringa.org.au](mailto:admin@baringa.org.au).

**7. Approval and Review Details**

| Approval and Review | Details           |
|---------------------|-------------------|
| Approval Authority  | Centre Management |
| Administrator       | Centre Director   |
| Next Review Date    | February 2024     |

| History                              | Details         |
|--------------------------------------|-----------------|
| Original Approval Authority and Date | 8 February 2021 |
| Amendment Authority and Date         | N/A             |
| Modifications made                   | N/A             |

## Appendix 1 Education and Care Services National Regulations

| Education and Care Services National Regulations |   |
|--|---|
| 168  | Education and care services must have policies and procedures                                 |
| 181  | Confidentiality of records kept by approved provider  |
| 195  | Application of Commonwealth Privacy Act 1988  |
| 196  | Modifications relating to National Education and Care Services Privacy Commissioner and Staff |

## Appendix 2 Resources

Australian Government Office of the eSafety commission [www.esafety.gov.au/early-years](http://www.esafety.gov.au/early-years)

eSafety Early Years Online safety for under 5s. <https://www.esafety.gov.au/sites/default/files/2020-02/Early-years-booklet.pdf>

eSmart Alannah & madeline foundation [www.esmart.org.au](http://www.esmart.org.au)

Family Tech Agreement. eSafety Early Years Online safety for under 5s

[https://www.esafety.gov.au/sites/default/files/2020-01/Our%20Family%20Tech%20Agreement\\_0.pdf](https://www.esafety.gov.au/sites/default/files/2020-01/Our%20Family%20Tech%20Agreement_0.pdf)

Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content: <https://www.kiddle.co/>

Receive information on scams that can then be provided to the public. To report an online scam or suspected scam, use the form found here: <https://www.scamwatch.gov.au/report-a-scam>

More information on online fraud and scams can be found on the Australian Federal Police website: <https://www.afp.gov.au/what-we-do/crime-types/cyber-crime/online-fraud-and-scams>

Notifiable Data Breaches scheme (NDB) can be made through the Australian Government Office of the Australian Information Commissioner

## Appendix 3 Source

Australian Children's Education & Care Quality Authority. (2014).

Australian Government eSafety Commission (2020) [www.esafety.gov.au](http://www.esafety.gov.au)

Australian Government Office of the Australian Information Commissioner (2019)

<https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/>

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).

Guide to the National Quality Standard. (2020).

*Privacy Act 1988.*

Revised National Quality Standard. (2018).