2.18 Cyber-bullying Policy

The service acknowledges it has a responsibility and Duty of Care to ensure that the rights of employees, volunteers, children, and families to be physically, emotionally, and psychologically safe whilst participating in on-line/internet activities associated with the service, are protected. This responsibility may extend beyond service on-line/internet activities, where such inappropriate behaviour, impacting harmfully upon employees, volunteers, children, and families, becomes known.

This policy aims to articulate the rights and responsibilities of employees, volunteers, children, and families associated with the service with regards to cyber-bullying.

Relevant Laws and other Provisions

The laws and other provisions affecting this policy include:

- *Education and Care Services National Law Act, 2010 and Regulations 2011*
- *Online Safety Act 2021 and Online Safety Amendment (Social Media Minimum Age) Bill 2024*
- Cyberbullying Scheme Regulatory Guidance updated January 2025
- *Family and Child Commission Act 2014*
- *Child Protection Act 1999 and Child Protection Regulations 2000*
- *Work Health and Safety Act 2011*
- *Duty of Care*
- *National Quality Standard 2.2 Each child is protected; National Quality Standard, Quality Area 5 – Relationships with children*
- *Policies: 2.2 – Statement of Commitment to the Safety and Wellbeing of Children and the Protection of Children from Harm, 2.8 – Anti-Bullying, 2.15 – Children's Property and Belongings, 2.16 – Promoting Protective Behaviours, 3.1 – Educational Program Planning, 6.2 – Provision of Resources and Equipment, 9.3 – Communication with Families, 10.9 – Risk Management and Compliance, 10.12 – Information and Technology.*

Procedures

Definitions

'ICT' - information and communication technology.

'Generative AI technologies' - is a type of artificial intelligence that can create new content, such as text, images, videos, and music, from existing data. Platforms include, but are not limited to, Open AI ChatGPT, Google Gemini, etc.

'Deepfakes' - A deepfake is a digital photo, video or sound file of a real person that has been edited to create an extremely realistic but false depiction of them doing or saying something that they did not actually do or say.

'Cyber-bullying' - involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others.

Cyber-bullying might occur over the internet, in instant messaging (IM), chat rooms, social networking sites, blogs, gaming sites, over the phone by SMS or MMS, by email or via other technologies.

While cyber-bullying is like real life bullying, it differs in the following ways:

- It is invasive and can occur 24/7 with a person being targeted at home, work or anywhere.
- It can involve harmful material being widely and rapidly disseminated to a large audience. For example, rumours and images [including deepfake alterations] can be posted on public forums or sent to many people at the 'press of a button;' and
- It can provide the bully with a sense of anonymity and distance from the victim so there is a lack of immediate feedback or consequences.

'E-crime' - occurs when a computer or other electronic communication device (e.g., mobile phone) is used to commit an offence, is targeted in an offence, or acts as a storage device to an offence.

Service Responsibilities

The service will ensure families are aware of the cyber-safety practices encouraged at any time employees, volunteers, children, or families are accessing ICT equipment or devices at the service.

The service understands that cyberbullying is a serious issue and always evolving as new technology and artificial intelligence technologies advance and are used for offensive means.

To preserve children's privacy, the Coordinator/Responsible Persons will limit the posting of images of children in the service to the Xplor/Playground platform. Only active families of the service will have access to these applications. This may include ensuring that confidential information is not accessible on publicly available websites and that images posted do not include any identifying images of the children without prior written permission from their parent/guardian as noted on their enrolment.

The service will ensure all educators are made aware of how to manage instances of cyber-bullying when children are accessing ICT equipment and devices.

Strategies and guidelines will be developed, in collaboration with the children, for using the ICT equipment and devices respectfully whilst in attendance at the service. This may include the development of 'user agreements,' in collaboration with educators, children, and families.

In consultation with management, if there is suspicion that an e-crime has been committed, the Coordinator /Responsible person will report it to the police. Where there is further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device, the device will be confiscated and handed to the investigating police officer. The electronic device should not be tampered with.

The service may also be required to complete a 'Notification of Serious Incident' form and forward it to the Regulatory Authority.

Educator Responsibilities

Educators will ensure their own practices role model appropriate safety measures when researching information, either individually or with the children.

Educators will ensure children are only able to access the internet at the service through authorised computers and/or mobile devices that have been fitted with appropriate security and filtering software.

Educators will encourage children's safe use of the internet, through implementing the following cyber-safe practices whilst participating in service-related activities:

- Never post personal information such as address or telephone number online.

- Never posting photos of themselves (such as 'selfies') online.
- Not responding to any messages that are mean or in any way makes them feel uncomfortable.
- Not sending any messages that may be mean or make another person feel uncomfortable.
- Never agreeing to meet any person they have met online.
- Never give their internet username or passwords to another person (even best friends).
- Checking with an educator before downloading or installing any software or games; and
- Informing an educator if they access information makes them feel uncomfortable.

Family Responsibilities

Informing the Coordinator /Responsible Person of any concerns you may have regarding cyber-safety and your child, whether it is happening at the service or not.

Be aware of your child's access to data on devices, whether securely connected through the service or accessible on their own device.

Encouraging your child to share information, including social networking sites (Facebook) with you as a 'friend' to monitor their safety online.

References

eSafety Commissioner, Australian Government. Cyberbullying Scheme Regulary Guidance (January 2025) https://www.esafety.gov.au/sites/default/files/2025-01/Cyberbullying-Scheme-Regulatory-Guidance-Updated-January2025_0.pdf?v=1747619264780

Dolly's Dream. Generative Artificial Intelligence and Cyber Bullying (March 2024). https://www.dollysdream.org.au/blog/generative-artificial-intelligence-and-cyber-bullying

Cyberbullying Research Centre (2025). https://cyberbullying.org/

DATE DEVELOPED	DATE RATIFIED	DATE REVIEWED	DATE RATIFIED
August 2018	August 2018	March 2021	May 2021
		February 2022	July 2022
		May 2025	June 2025