CYBER SAFETY POLICY

Cyber safety is the safe and responsible use of Information and Communication Technologies (ICT). It involves being respectful of other people online, using good 'netiquette' (internet etiquette), and above all, is about keeping information safe and secure to protect the privacy of individuals. Our Service is committed to create and maintain a safe online environment with support and collaboration with staff, families and community.

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
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.

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

RELATED LEGISLATION

Child Care Subsidy Secretary's Rules 2017	Family Law Act 1975
A New Tax System (Family Assistance) Act 1999	Family Assistance Law – Incorporating all related legislation for Child Care Provider Handbook in Appendix G https://www.dese.gov.au/resources-child-care-providers/resources/child-care-provider-handbook

RELATED POLICIES

CCS Data Policy CCS Personnel Policy CCS Governance Policy Code of Conduct Policy Dealing with Complaints Policy Enrolment Policy Family Communication Policy	Fraud Prevention Policy Personnel Policy Privacy and Confidentiality Policy Programming Policy Photography Policy Record Keeping and Retention Policy Technology Usage Policy

PURPOSE

To create and maintain a cyber safe culture that works in conjunction with our Service philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

SCOPE

This policy applies to children, families, educators, staff, visitors, approved provider, nominated supervisor and management of the Service.

TERMINOLOGY	
ICT	Information and Communication Technologies
Cyber safety	Safe and Responsible use of the internet and equipment/devices, including mobile phones and devices.
Netiquette	The correct or socially acceptable way of using the internet.

IMPLEMENTATION

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.

Our Service 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 daily reports, observations, photos, portfolios and email communications.

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

Educational Software Program

Our Service uses Xplor which is a password protected private program for 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.

Educators are alerted via Storypark and on their dashboard when a family member has added a comment. Likewise, families are notified when a relevant educator has posted a photo/comment about their child.

Access to a child's information and development is only granted to a child's primary guardians. No personal information is shared with any third party.

CCS Software

Our Service uses Xplor which is a third-party software system to access the Child Care Subsidy System (CCSS). The software is used to manage the payment and administration of the Child Care Subsidy (CCS).

Review of CCS software: The Approved Provider will ensure the CCS software has policies and procedures regarding safe storage of sensitive data before using the software, the Approved Provider will review the privacy policy of the CCS software on a yearly basis or as required. The Approved Provider will review any potential threats to software security on a monthly/ yearly basis. The Director/ Nominated Supervisor will advise the Approved Provided as soon as possible regarding any potential threat to security information and access to data sensitive information. Any breaches of data security will be notified to the Office of the Australian Information Commissioner (OAIC) by using the online Notifiable Data Breach Form.

All Personnel using the software will have their own log in username and password.

The Approved Provider will ensure all Personnel using the software will have their own log in username and password. Authorised users are encouraged to change their passwords every 6 months.

Each Personnel who is responsible for submitting attendances and enrolment notices to CCSS will be registered with PRODA as a Person with Management or Control of the Provider or as a Person with Responsibility for the Day-to-Day Operation of the Service.

The Approved Provider will review staff log ins on a monthly/ yearly basis and ensure this procedure is followed by all staff who access CCS software to submit data to CCS.
See: *Cyber Safety Procedure*

Review of CCS Software Procedure:

Review	How often	By Whom
All staff use an individual log-in to access CCS software	Upon employment Yearly As required	Approved Provider and Director/ Nominated Supervisor
Privacy policy of CCS software	Initial access to CCS software Yearly As required	Approved Provider
Any breaches of sensitive data relating to Enrolments	Upon notification	Approved Provider

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 the Service's network or any device
- privacy laws are such that educators or other employees should seek advice from Service 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 the Service Internet/Intranet site should be appropriate to the Service's learning environment
- material can be posted only by those given the authority to do so by the Service management.

- the Service management should be consulted regarding links to appropriate websites being placed on the Service's Internet/Intranet (or browser homepages) to provide quick access to sites.

MANAGEMENT WILL ENSURE:

- all staff, families and visitors are aware of the Service's *Code of Conduct* and *Confidentiality and Privacy Policies.*
- the Service works with an ICT security specialist to ensure the latest security systems are in place to ensure best practice. 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.
- backups of important and confidential data are made regularly (monthly is recommended)
- backups are stored securely either offline, or online (using a cloud-based service)
- software and devices are updated regularly to avoid any breach of confidential information
- families are referred to the *Dealing with Complaints Policy* and procedure when raising concerns regarding digital technologies and personal data
- all staff are aware that a breach of this policy may initiate appropriate action including the termination of employment.

NOMINATED SUPERVISOR/ RESPONSIBLE PERSON / EDUCATORS WILL:

- ensure to use appropriate netiquette and stay safe online by adhering to Service policies and procedures
- keep passwords confidential and not share with anyone
- log out of sites to ensure security of information
- never request a family member's password or personal details via email, text, or Messenger
- 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)
- obtain parent permission for children to use computers as part of the enrolment procedure
- ensure that children are never left unattended whilst a computer or mobile device is connected to the internet
- ensure personal mobile phones are not used to take photographs, video or audio recordings of children at the Service
- only use educational software programs and apps that have been thoroughly examined for appropriate content prior to allowing their use by children.
- provide parents and families with information about the apps or software programs accessed by children at the Service

- participate in professional development regarding online safety
- ensure that appropriate websites are sourced for use with children **prior** to searching in the presence of children
- use a search engine such as 'Kiddle' rather than Google to search for images or information with children (See 'Resources' section)
- ensure privacy filters and parental control settings are turned on and used when children are accessing digital technologies online
- 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 the Service or if the device is left behind whilst on an excursion

FAMILIES

- 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.
- When it comes to your own children, it is your choice what you share outside of the Service. 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.
- Be mindful of what you publish on social media about your child as this may form part of their lasting digital footprint.
- Install Family Friendly Filters to limit access to certain types of content on devices such as mobile phones and computers.
- Install parental controls on streaming services to ensure children are not able to access inappropriate material.
- Consider developing a *Family Tech Agreement* to establish rules about use of devices at home.
- Sometimes other children in the Service 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.
- Access further information about eSafety to help protect your children and be cyber safe.

RESOURCES

Australian Government Office of the eSafety commission 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

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

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

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

SOURCE

Australian Children's Education & Care Quality Authority. (2014).
Australian Government eSafety Commission (2020) www.esafety.gov.au
Australian Government Department of Education, Skills and Employment. *Child Care Provider Handbook (2018)*
https://www.dese.gov.au/resources-child-care-providers/resources/child-care-provider-handbook
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).
Education and Care Services National Law Act 2010. (Amended 2018).
Education and Care Services National Regulations. (2011).
Guide to the Education and Care Services National Law and the Education and Care Services National Regulations. (2017).
Guide to the National Quality Framework. (2017). (Amended 2020).
Guide to the National Quality Standard.
Privacy Act 1988.
Revised National Quality Standard. (2018).

REVIEW

POLICY REVIEWED BY	TRACEY DAVEY	OPERATIONS MANAGER	MARCH 2022
POLICY REVIEWED	MARCH 2022	NEXT REVIEW DATE	MARCH 2023
MODFICATIONS	• Edits to ensure adherence to CCS data protection • Addition of Dealing with Complaints Policy • Parental controls- privacy filters added • Sources checked		

POLICY REVIEWED	PREVIOUS MODIFICATIONS	NEXT REVIEW DATE
AUGUST 2021	• Sources checked and links updated • Additional reference added for CCS Provider Handbook • Updated Related legalisation	MARCH 2022
MARCH 2021	• review of policy to align to 2021 schedule • sources checked for currency	MARCH 2022
OCTOBER 2020	• Additional information added regarding CCS Software security • policy reviewed	MARCH 2021
MARCH 2020	• Additional content added • Additional information added to Family section • Resources added	MARCH 2021
OCTOBER 2019	• Notifiable Data Breach Scheme information added • Re-worded introduction • Resources section added • Additional information added to points • Sources checked for currency • Sources alphabetised	MARCH 2020
MARCH 2018	• Updated to comply with changes to the Australian Privacy Act	MARCH 2019
NOVEMBER 2017	• Updated Policy to comply with the revised National Quality Standard	MARCH 2018
MARCH 2017	• Reviewed policy, no changes made.	MARCH 2018