CYBER SAFETY PROCEDURE

Montessori Early Learning Seacliff is committed to create and maintain a safe online environment with support and collaboration with staff, families and community. This procedure will ensure the safe and responsible use of Information and Communication Technologies (ICT) within our Service. All staff will follow this procedure and be respectful of other people online, use good 'netiquette' (internet etiquette) and keep information safe and secure to protect the privacy of individuals.

Working in conjunction with the *Cyber Safety Policy*, this procedure aims to protect children, staff and the Service from risks associated with digital technology and online activities, including privacy and bullying breaches.

Education and Care Services National Law or Regulations *(R.84, 168, 181, 195 and 196) NQS QA 2: Element 2.1.2, 2.2.1, 2.2.3 and 7.1.2. Health and Governance practices and procedures*
Related Policies: *Cyber Safety Policy, Privacy and Confidentiality Policy and Code of Conduct*

STEP 1: EDUCATIONAL SOFTWARE PROGRAM		
The nominated supervisor/responsible person/educators will:		
1	obtain parent authorisation for children to use computers as part of the enrolment procedure	
2	ensure that children are supervised if utilising a computer or mobile device is connected to the internet	
3	only use educational software programs and apps that have been thoroughly examined for appropriate content prior to allowing their use by children	
4	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.	
5	provide parents and families with information about the apps or software programs accessed by children at the Service	
6	advise 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	

STEP 2: CCS SOFTWARE		
1	Each person 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	
2	All provider personnel using Xplor Education will have their details updated as required in the software- [personal details, date of birth, address, email, phone number, Working with Children's Check, Supporting Documentation-Australian Police Criminal History Check, declaration- Australian Securities and Investments Commission (ASIC), National Personal Insolvency Index check]	
3	All provider personnel will use their own secure log on username and password	
4	Personnel will not share their log on at any time	

STEP 3: CONFIDENTIALITY AND PRIVACY		
1	Educators or staff will 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)	
2	Parents/guardians will be requested to sign an authorisation form to ensure children's privacy, safety and copyright associated with the online publication of children's personal details, images, videos or work. If authorisation is not provided the child's personal details, images, videos or work will not be published online.	
3	All material submitted for publication on the Service Internet/Intranet site will be appropriate to the Service's learning environment	
4	Material will only be posted by those persons given the authority to do so by the Service management	
5	Service management will be consulted regarding links to appropriate websites being placed on the Service's Internet/Intranet (or browser homepages) to provide quick access to sites	
6	All staff, families and visitors will be made aware of the Service's *Code of Conduct and Privacy and Confidentiality Policies*	
7	Management/nominated supervisor/responsible person/educators will: • 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 other method	

STEP 4: SECURITY SYSTEMS		
Management will:		
1	Be aware of and take reasonable steps to ensure the latest security systems are in place to ensure best practice	
2	ensure staff are trained on how to avoid unsuitable content on the internet	
Management and educators will:		
3	report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes staff/educators feel uncomfortable (See '*Cyber Safety Policy*' section for where to report)	
4	ensure that appropriate websites are sourced for use with children prior to searching in the presence of children	
5	Approach online searching with caution to avoid accessing unsuitable content	

STEP 5: BACKUPS AND UPDATES		
Management will ensure:		
1	backups of important and confidential data are made regularly	
2	backups are stored securely either offline, or online (using a cloud-based service)	
3	software and devices are updated regularly to avoid any breach of confidential information	

STEP 6: BREACHES AND NOTIFICATIONS		
1	The nominated supervisor will report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes you feel uncomfortable (See '*Cyber Safety Policy*).	
2	The nominated supervisor will 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.	
3	Management will conduct a *Privacy Audit* to ensure ongoing compliance with privacy obligations and recent changes. The *Privacy Audit* should be completed on a yearly basis or following any breaches in data at the service. The *Privacy Audit* will assist Services to: - Identify how to meet privacy obligations - Identify how to improve on existing privacy management - Identify potential areas of privacy risk - Alleviate these risks by improving compliance with the Privacy Act	
4	Services are required to have a Data Breach Response which sets out procedures in the event of a data breach (or suspected data breach). A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. A *Data Breach Response Plan* will enable management to contain, evaluate the risks, consider the breach and review and respond to a data breach.	

REVIEW OF PROCEDURE			
Date procedure created	27 May 2025	To be reviewed	27 May 2026
Approved by	Jason Williams	Signature	
Procedure Reviewed Date	Modifications/Changes		

Document originally created using Childcare Centre Desktop: V5.02.25