CYBER SAFETY PROCEDURE

Our Service 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 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

Education and Care Services National Law or Regulations (R.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		
Director/Nominated Supervisor/Responsible Person/educators will:		
1	Obtain parent permission for children to use computers as part of the enrolment procedure	
2	Ensure that children are never left unattended whilst 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 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 will sign a permission to publish form to ensure children's privacy, safety and copyright associated with the online publication of children's personal details or work	
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	Director/ 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 Messenger	

STEP 4: SECURITY SYSTEMS		
1	Management will: • work with an ICT security specialist to ensure the latest security systems are in place to ensure best practice. • ensure anti-virus and internet security systems including firewalls can block access to unsuitable web sites, newsgroups and chat rooms	
2	Management will: • 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) • ensure that appropriate websites are sourced for use with children prior to searching in the presence of children	
3	Management and educators will: • use a search engine such as 'Kiddle' rather than Google to search for images or information with children (See 'Resources' section in policy).	

STEP 5: BACKUPS AND UPDATES		
1	Management will ensure: • backups of important and confidential data are made regularly (monthly is recommended)	
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	Director/ 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	Director/ 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	It is recommended that management 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 Plan* 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.	