DATA SECURITY PROCEDURE AND CHECKLIST

Privacy is acknowledged as a fundamental human right. All employees will maintain confidentiality of personal and sensitive information to foster positive trusting relationships with families. We aim to protect the privacy and confidentiality of all information and records about individual children, families, educators, employees and management by ensuring continuous review and improvement on our current systems, storage, and methods of disposal of records. By including data security in our induction and orientation program we aim to raise awareness of employee responsibilities and have all employees contribute to maintaining a secure data environment within the service. Data security is carefully considered when employees resign or leave a service, to prevent any unauthorised access or misuse of sensitive or confidential information.

Working in conjunction with the *CCS Data Security Policy, Privacy and Confidentiality Policy and Privacy and Confidentiality Procedure*, this procedure and checklist provides guidance to ensure data is stored, used and accessed in accordance with relevant policies and procedures.

Education and Care Services National Law or Regulations *(R.168, 170, 171, 177, 181, 183 and 184) NQS QA 7: Element 7.1, 7.1.1, 7.1.2, 7.1.3 and 7.2 Governance practices and procedures*
Related Policy: *Privacy and Confidentiality Policy and CCS Data Security Policy*

INDUCTION PROCEDURE		
1	The approved provider, nominated supervisor and employees will review the Service's *CCS Data Security Policy* and *Privacy and Confidentiality Policy* annually	
2	All new employees using CCS Software will register with PRODA and complete relevant background checks	
3	New employees will be required to sign a *Confidentiality Agreement* as part of their induction and orientation	
4	New employees will be provided information and guidelines on how to access, handle, store and transmit data securely	
5	New employees are to be aware of the *Privacy Law Compliance Procedure* and follow the procedure for any breaches of data security	
6	New employees are to be informed of password management, including any password management system the service implements. Employees are expected to create strong passwords and to change passwords on a regular basis.	

7	New employees are advised of how the service stores physical and digital files. Employees are provided with any USB or Hard Drives to store data information securely if not cloud storage is not used.	
8	New employees will ensure they do not share their log on username or passwords at any time	

RESIGNATION/EXIT PROCEDURE		
1	Employees who provide resignation are informed of their responsibilities and obligations in relation to the *Confidentiality Agreement*	
2	Management will remove access to email address, SharePoint and/or cloud storage and folders to an employee who has ended employment	
3	Employees who have resigned are to provide any equipment or devices, including USBs or Hard Drives	
4	Employees who have resigned are to acknowledge not to access accounts or misuse sensitive or confidential information	
5	An *Employee Exit Checklist* is completed for all employees who have resigned from the service, in particular attention provided to the Data Security section	
6	Management will consult with the *Employee Exit Guide* to ensure all aspects of Data Security are considered when an employee provides resignation	

DATA SECURITY PROCEDURES		
1	Management and employees will ensure each computer and device used within the service has antivirus software installed, is applied at all times and is set to update automatically	
2	Management and employees will ensure software and operating systems are updated as patches and updates are available, including windows updated	
3	Management and employees will ensure backups of important and confidential data are made regularly	
4	Management and employees will ensure they log out of websites to ensure security of information	
5	Management and employees will report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes staff/educators feel uncomfortable	
6	Management and employees will ensure access to personal and sensitive information is restricted to key personal only	

DATA SECURITY CHECKLIST

Employee full name			
Start Date		Position	

ACCOUNT SET UP	DATE ACTIONED	DETAILS	PASSWORDS PROVIDED
Email address			
OneDrive			
Xero Software			
CCS Software – Xplor			
Password Management System			

ACKNOWLEDGEMENTS	DATE	SIGNATURE
I acknowledge I have read and understand the Service *Privacy and Confidentiality Policy* and *CCS Data Security Policy*		
I acknowledge I have read, understand and signed the *Confidentiality Agreement*		
I agree to update software and operating system programs as patches and updates are available, including Windows updates		
I agree to report any Data Breaches to management and where appropriate to OAIC as per *Privacy Law Compliance Procedure*		
I agree to inform management of any circumstances which may affect the fit and proper status, in particular in relation to CCS Management		
I agree to ensure antivirus software is installed and applied to service computers and devices at all times and set to automatic updates.		

Employee name		Date	
Employee signature			

Nominate supervisor name		Date	
Nominate supervisor signature			

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