CCS DATA SECURITY POLICY

This policy provides information regarding the processes relating to the administration of Child Care Subsidy (CCS) to families and ensures our Service is compliant and adhering to Family Assistance Law obligations as part of the service's ongoing approval under Family Assistance Law.

RELATED LEGISLATION

Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook https://www.education.gov.au/early-childhood/resources/child-care-provider-handbook
A New Tax System (Family Assistance) Act 1999
A New Tax System (Family Assistance) (Administration) Act 1999
Child Care Subsidy Minister's Rules 2017
Child Care Subsidy Secretary's Rules 2017
Child Care Subsidy (What Constitutes a Session of Care) Determination 2018
Corporations (Aboriginal and Torres Strait Islander) Act 2006
Education and Care Services National Law Act 2010
Education and Care Services National Regulations 2011
Family Law Act 1975
Fringe Benefits Tax Assessment Act 1986
Social Security Act 1991
Work Health and Safety Act 2011
Family Assistance Legislation Amendment (Jobs for Families Child Care Package) Act 2017

RELATED POLICIES

CCS Account Policy CCS Governance Policy CCS Notifications Policy CCS Personnel Policy Code of Conduct Policy	Cyber Safety Policy Fraud Prevention Policy Privacy and Confidentiality Policy Technology Usage Policy

PURPOSE

Our Service aims to comply with the Child Care Subsidy legislative requirements associated with operating a fee reduction service for eligible families, including assurance of data security used with third-party CCS software. Our Service aims to maintain the financial integrity of all child care funding by

submitting correct data at all times to the Department of Education through our CCS Software. Our Service will ensure all reporting requirements for claiming and administering CCS payments will be maintained.

SCOPE

This policy applies to families, staff, management, Approved Provider and Nominated Supervisor and authorised users of the CCS Software of the Service.

IMPLEMENTATION

Our *CCS Data Security Policy* provides guidance around third-party software security in relation to the administration and management of Child Care Subsidy and Additional Child Care Subsidy. Our Service uses Kidsoft to manage and interact with the Australian Government's Child Care Subsidy System.

This policy includes information about the CCS software program, the Services' obligations and responsibilities, and the nature of possible risks associated with internet use, including privacy and data breaches.

THIRD-PARTY SOFTWARE SECURITY

Our Service uses Kidsoft which is a password protected third-party software system for educators and staff at our Service who are authorised to interact with the CCS Software to manage and administer data information and payments associated with the Child Care Subsidy and Additional Child Care Subsidy.

The Approved Provider will determine personnel who is required to use the CCS Software System. All personnel who are authorised to use our CCS Software will be required to meet the fit and proper requirements as set by the Department of Education (see *CCS Personnel Policy* for further information regarding authorised personnel).

The Approved Provider will ensure all Personnel using the software will have their own log in username and password credentials to use the CCS Software. The login and password credentials will be linked to individual PRODA accounts as per Family Assistance Law. Authorised users are encouraged to change their passwords every 6 months.

The Approved Provider will audit staff log ins on a yearly basis and ensure this procedure is followed by all staff who access CCS software to submit data to CCS. The *CCS Compliance Checklist/ Audit* will be used

each month by the Approved Provider to review usernames of staff using CCSS Software and to review the privacy policy of individual CCS Software.

DATA INTEGRITY

The *Fraud Prevention Policy* and *Fraud Corruption Prevention Procedure* outlines that CCS Software will be monitored by the Approved Provider to ensure data integrity and security is maintained by all staff who process CCS payments to families. Attendances are cross referenced against child booking reports to ensure sessions are correct when submitted to CCS. Sessions which require resubmission are resubmitted to CCS within 14 days.

Reports generated by the CCS Software will be cross referenced against records kept at the service each month. Our Service implements processes and procedures to ensure the accuracy of data that is submitted through the CCS Software.

The Approved Provider will ensure all computers are password protected and each staff member uses their own log in and password credentials to access service information. The Approved Provider will determine personnel who is required to use the CCS Software System. All personnel who are authorised to use our CCS Software will be required to meet the fit and proper requirements as set by the Department of Education (see *CCS Personnel Policy* for further information regarding authorised personnel). Authorised personnel will be required to hold their own log in and password credentials to use the CCS Software.

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 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.

REVIEW OF CCS SOFTWARE PROCEDURE

REVIEW	HOW OFTEN	BY WHOM
All authorised users are to 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
Authorised users are encouraged to change their login credential passwords	Every 6 months (forced password change via Kidsoft)	Individual Users

CCS COMPLIANCE CHECKLIST

Our Service will use Kidsoft to ensure compliance of CCS payments to families.

The *CCS Compliance Checklist/Audit* will be completed each month by the Approved Provider together with staff who use the CCS software to administer CCS payments to families. This checklist is used as a tool to ensure the accuracy of data submitted to the Department of Education through our CCS Software in relation to CCS payments.

INDUCTION AND RESIGNATION OF STAFF

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. Management will refer to the *Data Security Procedure and Checklist* to ensure data is stored, used and accessed in accordance with relevant policies and procedures.

THE APPROVED PROVIDER/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 are in place

- 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
- all authorised Personnel using the software will have their own log in username and password
- 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.
- authorised users change their login credential passwords every 6 months

NOMINATED SUPERVISOR/ RESPONSIBLE PERSON / EDUCATORS WILL:

- keep passwords confidential and not share with anyone
- log out of sites to ensure security of information
- 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)
- provide families with information about the CCS Software which is used to maintain CCS information and payments.
- 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 or family member is mistakenly given to the wrong person

CCS DATA SECURITY PROCEDURES

STEP 1: CCS SOFTWARE		
1	The Approved Provider will ensure 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	The Approved Provider will ensure all Provider Personnel using Kidsoft 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	The Approved Provider will ensure all authorised Personnel will use their own secure log on username and password to access CCS Software	

4	The Approved Provider will ensure Personnel will not share their log on username or password at any time	
5	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 another staff member's log in/ password or personal details regarding CCS Software	
6	Authorised users change their passwords every 6 months.	

STEP 2: SECURITY SYSTEMS, BACKUPS AND UPDATES		
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 are in place	
2	Management and educators will report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes staff/educators feel uncomfortable	
3	Management will ensure: • 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.	

STEP 3: 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	
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 data base or CCS Software with personal information about children and/or families is hacked • personal information about a child is mistakenly given to the wrong person This applies to any possible breach within the Service or if the CCS Software is hacked from an online source	
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.	

CCS DATA INTEGRITY PROCEDURE

STEP 1: CCS SOFTWARE		
1	All authorised users of CCSS software have attended training to correctly use the CCS Software	
2	All authorised personnel and users of CCSS Software are aware of and understand the CCS Provider Handbook.	
3	All personnel involved in the administration of CCS payments to families understand their legal obligations in relation to the administration of CCS	
4	The Approved Provider will conduct an audit using the CCS Compliance Checklist/Audit to ensure the accuracy of data submitted to the Department of Education through our CCS Software in relation to CCS payments.	
5	The Approved Provider will ensure all authorised Personnel will use their own secure log on username and password to access CCS Software	
6	The Approved Provider will ensure Personnel will not share their log on username or password at any time	
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 another staff member's log in/ password or personal details regarding CCS Software	
8	Attendances are cross referenced against child booking reports to ensure sessions are correct when submitted to CCS.	
9	Sessions which require resubmission are resubmitted to CCS within 14 days	
10	CCS payments are checked by the financial officer each month and any anomalies are discussed with the Approved Provider and Director/ Nominated Supervisor.	
11	CCS Payment reports and invoices are electronically stored each week for future cross referencing and checking.	

RESOURCES

Australian Government Office of the eSafety commission www.esafety.gov.au/early-years

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

CONTINUOUS IMPROVEMENT/REFLECTION

Our *CCS Data Security Policy* will be updated and reviewed annually in consultation with families, staff, educators and management.

CHILDCARE CENTRE DESKTOP- RELATED RESOURCES

CCS Compliance Checklist / Audit CCS Application Guide CS Procedures Guide	Data Breach Response Procedure Data Security Procedure and Checklist

SOURCES

Australian Government eSafety Commission (2020) www.esafety.gov.au
Australian Government Department of Education. *Child Care Provider Handbook. (2022)* https://www.education.gov.au/early-childhood/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/
Education and Care Services National Law Act 2010. (Amended 2023).
Education and Care Services National Regulations. (2011). (Amended 2023).
Guide to the National Quality Framework. (2017). (Amended 2023).
Privacy Act 1988.
Western Australian Education and Care Services National Regulations

REVIEW

POLICY REVIEWED BY	Peter Colliver	Approved Provider	May 2024
POLICY REVIEWED	JULY 2023	NEXT REVIEW DATE	NOVEMBER 2024
VERSION	V4.07.23		

MODIFICATIONS	• Removal of CCS Compliance Checklist information • Sources updated and links edited	
POLICY REVIEWED	PREVIOUS MODIFICATIONS	NEXT REVIEW DATE
SEPTEMBER 2022	• Update of Department name from Department of Education, Skills, and Employment to **Department of Education** • minor formatting edits within text • hyperlinks checked and repaired as required • link to Western Australian Education and Care Services National Regulations added in 'Sources' • links within policy updated from DESE.gov.au to education.gov.au • Continuous Improvement/Reflection section added • Childcare Centre Desktop Resource section added	NOVEMBER 2023
OCTOBER 2021	• New Policy Developed	OCTOBER 2022