POLICY IN THIS SECTION AS REQUIRED BY:

Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook in 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

PURPOSE:
The 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. The Service aims to maintain the financial integrity of all childcare funding by submitting correct data at all times to the Department of Education through our CCS Software. The 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, Nominated Supervisors and authorised users of the CCS Software of the Service.

POLICY:
The Service Data Protection Policy provides guidance around third-party software security in relation to the administration and management of Child Care Subsidy and Additional Child Care Subsidy. The Service uses Harmony Software to manage and interact with the Australian Government's Child Care Subsidy System.
Harmony Software is a password protected third-party software system for Educators and staff who are authorised to interact with the Child Care Subsidy System (CCSS). The software is used to manage and administer data information and payments associated with the administration of the Child Care Subsidy (CCS) and Additional Child Care Subsidy.
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.

PROCEDURES:
The Approved Provider will:
1. 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.
2. 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.

DATA INTEGRITY:
The Fraud Prevention Policy 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.

PROCEDURES:
1. Reports generated by the CCS Software will be cross referenced against records kept at the service each week. Our Service implements processes and procedures to ensure the accuracy of data that is submitted through the CCS Software. The Office Manager will complete the *CCS Compliance Checklist/ Audit* each month to identify any data anomalies within incorrect data submissions are picked up in a timely manner. Any anomalies will be reported to the Approved Provider. The checklist is used as a tool to facilitate fraud prevention and detection within our Service in relation to correct data entry for enrolments, attendances, CCS payments, personnel, and record keeping.
2. CCS payments are checked by the administration staff each week and any anomalies are discussed with the Approved Provider and Managers/ Nominated Supervisor. CCS Payment reports and invoices are electronically stored each week for future cross referencing and checking.
3. 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.
4. The Approved Provider will determine personnel who is required to use the CCS Software System.
5. Authorised personnel will be required to hold their own log in and password credentials to use the CCS Software. The log in and password credentials will be linked to individual PRODA accounts as per Family Assistance Law.

REVIEW OF CCS SOFTWARE:

1. 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.
2. The Approved Provider will review any potential threats to software security on a yearly basis.
3. The Manager/ 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.

CCS COMPLIANCE CHECKLIST

Our Service will use Harmony Software to ensure compliance of CCS payments to families. The *CCS Compliance Checklist/Audit* will be completed each month by the Office Manager together with staff who use the CCS software to administer CCS payments to families. Any

anomalies will be reported to the Approved Provider. 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 staff and Educator responsibilities and have all staff and Educators contribute to maintaining a secure data environment within the service.
Data security is carefully considered when staff or an Educator resigns or leaves a service, to prevent any unauthorised access or misuse of sensitive or confidential information.

PROCEDURE

THE APPROVED PROVIDER/MANAGEMENT WILL ENSURE:

1. All Educators, staff, families and visitors are aware of the Service's Code of Conduct and Confidentiality, Privacy and Educator Record Management Policy.
2. The Service works with an Information and Communications Technology (ICT) security specialist to ensure the latest security Systems are in place to ensure best practice. Anti-virus, internet security systems including firewalls and external monthly maintenance checks are in place
3. Backups of important and confidential data are made weekly
4. Backups are stored securely offline and online (using a cloud-based service) software and devices are updated regularly to avoid any breach of confidential information
5. All authorised Personnel using the software will have their own log in username and password
6. 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.
7. Authorised users change their login credential passwords every 6 months
8. When a staff member who has access to the Service date leaves, their login systems will be deleted and their authorisation in PRODA removed

NOMINATED SUPERVISOR/RESPONSIBLE PERSON/FAMILY DAY CARE EDUCATORS WILL:

1. Keep passwords confidential and not share with anyone
2. Log out of sites to ensure security of information
3. 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)
4. Provide families with information about the CCS Software which is used to maintain CCS information and payments.
5. 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

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

Dunsborough Computers www.dunsboroughcomputers.com.au

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