POLICY/ PROCEDURE NAME & REVIEW PROCESS	**CCS -CYBER SAFETY POLICY** This policy and procedure has been created to provide all stakeholders with clear guidelines and transparency to our practices and procedures. We welcome feedback and input from all stakeholders at any time and this policy is subject to review based on feedback or due date of annual review.
NATIONAL QUALITY STANDARD	**QUALITY AREA 7 GOVERNANCE AND LEADERSHIP** **7.1 GOVERNANCE** 7.1.2 Management systems. 7.1.3 Roles and responsibilities.
NATIONAL LAW AND REGULATIONS	170-Policies and procedures to be followed 171-Policies and procedures to be kept available 172- Notification of change to policies or procedures
RELATED POLICIES and RECORDS	▪ Enrolment Record ▪ Media Alert Record ▪ National Model Code Policy ▪ Privacy and Confidentiality Policy. ▪ Technology Policy
SCOPE OF POLICY	This policy applies to approved provider, nominated supervisor, employees, educators, families, students, volunteers, and visitors to the service.
AIM OF POLICY	To ensure that the service has strong guidelines, procedures, and practices in place regarding cyber safety. The aim of this policy is to ensure that the service staff adheres to Family Assistance Law by implementing robust cyber safety measures. This includes safeguarding the privacy and security of personal and sensitive information related to families and children. Our aim is to provide a clear policy, implement the policy, support practices relating to the policy, train staff regarding the policy and maintain and update the compliance of the policy for all our stakeholders.
SERVICE IMPLEMENTATION	**Implementation** Australia has stringent data protection laws, and childcare services are expected to adhere to these regulations. Failure to comply can lead to hefty fines and legal action. But beyond the legal implications, there's a moral duty to protect the sensitive information of the families who rely on your services. Protecting this data is not just a legal obligation, but a moral one. The trust parents place in the service to safeguard their children also extends to their data. Cyber safety is also about protecting all employees and children in the service when they are using technology such as laptops, iPad, computers. In conjunction with the *technology policy* and *national model code policy* all employees of the service will be guided and monitored to ensure compliance of cyber safety. In order to protect children, the approved provider in conjunction with the nominated supervisor will ensure that families are made aware of the services policies and procedures to: ▪ Protect personal information and privacy of children, families, and staff. ▪ Advise them on safe and appropriate use of the internet and digital devices. ▪ Educate children, staff, and families about cyber safety. ▪ Prevent and respond to cyberbullying, online harassment, and other cyber threats. **In regard to CCS Software** An approved provider under Family Assistance Law is responsible and must meet obligations under both Commonwealth and state and territory laws. They must comply with Family Assistance Law, comply with the National Law and National Regulations, and ensure the relevant personnel are fit and proper persons to engage in the process of receiving and passing on of Childcare Subsidy payments. They must complete background checks, including criminal history and working with children checks. The service will use a third-party software that is competent in CCS administration payments and data collection. **Further measures will include the following:** ▪ Protecting personal and sensitive information from unauthorised access or disclosure through the use of complex, hard to guess passwords (example: a combination of numbers, upper and lowercase letters, and symbols and/or phrases with a minimum of eight characters) ▪ Ensure that all employees who have access to sensitive data are fit and proper persons who are registered with PRODA as a person with management control of the provider or as a person with

Policy Name	**CCS- CYBER SAFETY POLICY**			Policy Version	V.2
Owner	Fishbowl Service Support Pty Ltd				
Policy published	August 2024	Last review date	August 2025	Next review date	August 2026

Service Support Within Reach Warning -uncontrolled when printed. This document is current at the time of printing and may be subject to change without notice

Page | 1

responsibility for the day-to-day operation of the service and will have individual password that they do not share with other employees.

- Will regularly update staff passwords and use secure authentication methods.
- Will install antivirus software on all the service technology equipment.
- Will have a system in place to ensure that all CCS data is backed up and stored securely.
- Will ensure that all approved staff receive training in implementing service software.
- All data will be backed up and stored appropriately and securely on a regular basis.
- Regular audits of software and staff practices to ensure compliancy.

Each member of the team plays an important role in the implementation of each policies guidelines, and they are outlined as below but not limited to the following:

The Approved Provider
- Will ensure written consent or denial regarding publishing photos of children will be in the *enrolment record* and families will be instructed about this consent prior to enrolment and be advised of the social media platforms that are used by the service.
- Will ensure that there is a copy of the *media alert record* in all rooms and that all staff are aware of it.
- Will ensure that all staff and families are aware of the services *privacy and confidentiality policy.*
- Will ensure that any employees appointed to one of the roles responsible for the implementation of CCS is suitably qualified and has all the appropriate qualifications and checks in place.
- Will ensure that fees are set for families and will ensure 14 days' notice is given to families via email online, memos etc to advise of fee increases.
- Will ensure that all computers used in the service are maintained with up-to-date antivirus software and firewall protection.
- Ensure staff complete cybersecurity induction and annual refreshers.
- Will ensure that copies of the policy and procedures are readily accessible to nominated supervisors, educators, staff, volunteers, and families, and are available for inspection.
- Will notify families at least 14 days before changing the policy or procedures if the changes will.
    - Affect the fees charged or the way they are collected or
    - Significantly impact the service's education and care of children or
    - Significantly impact the family's ability to utilise the service.
- Will ensure that obligations under the Education and Care Services National Law and National Regulations are met.
- Will ensure they take reasonable steps to ensure that the nominated supervisor, educators, staff, and volunteers follow the policy and procedures.
- Will ensure they provide the nominated supervisor, educators, staff and volunteers the documentation to perform their role, follow policy, procedure, and document according to regulatory and service requirements.
- Will ensure that adequate induction process is provided to all staff to ensure they have time to read and understand policies and procedures and seek further information if unsure.
- Will ensure that the nominated supervisor and staff are equipped with ongoing professional development and training they require to comply with this policy.
- Will encourage feedback from stakeholders regarding the policy's effectiveness, particularly in relation to identifying and responding to child safety concerns.
- Will ensure the policy is kept up to date with current legislation, research, and best practice.

The Nominated Supervisor
- Will monitor and ensure that any employees appointed to one of the roles responsible for the implementation of CCS is suitably qualified and has all the appropriate qualifications and checks in place. They will check expiry dates and advise approved provider of any variations of compliance actions against their employees.
- Will provide regular training for staff on cyber safety, including recognising online threats, safe practices, and how to handle cyberbullying.
- Will develop a plan for responding to data breaches or cyber incidents, including notifying affected individuals and authorities if necessary.
- Will ensure that when families are orientating that they are made aware information about the apps or software programs accessed by children at the service.

Policy Name	**CCS- CYBER SAFETY POLICY**			Policy Version	V.2
Owner	Fishbowl Service Support Pty Ltd				
Policy published	August 2024	Last review date	August 2025	Next review date	August 2026

Service Support Within Reach   Warning -uncontrolled when printed. This document is current at the time of printing and may be subject to change without notice

Page | 2

- Will monitor the use of software according to the *national model code policy* and conduct checks on the correct implementation of all staff practices.
- Will establish guidelines for staff regarding the use of social media, particularly concerning interactions with families and the sharing of professional information.
- Will put in place a risk assessment to identify and address potential vulnerabilities in the services technology and practices and will review on a yearly basis or earlier if areas of concern are identified.
- Will ensure all staff are made aware of *National model code policy, technology policy, privacy, and confidentiality policy.*
- Will adhere to and implement the obligations under the Education and Care Services National Law and National Regulations.
- Will ensure they take reasonable steps to ensure that the educators, staff, and volunteers follow the policy and procedures.
- Will ensure they provide the educators, staff and volunteers the documentation to perform their role, follow policy and procedure and ensure they are checking the documentation according to regulatory and service requirements.
- Will ensure that a rigorous recruitment process is completed, and a thorough induction process is provided to all staff to ensure they have time to read and understand policies and procedures and seek further information if unsure.
- Will ensure that the staff are supported with ongoing professional development and training they require to comply with this policy.
- Will encourage feedback from stakeholders and staff regarding the policy's effectiveness, particularly in relation to identifying and responding to child safety concerns.
- Will ensure the policy is kept up to date with current legislation, research, and best practice.
- Will conduct regular staff meetings to address policy compliance with legislation, policy implementation, changes to policy and or collect feedback for annual review of policy.

Educators

- Will teach children about safe internet practices, including not sharing personal information, recognising online threats, and reporting any suspicious behaviour.
- Will ensure that children are never left unattended whilst a computer or mobile device is connected to the internet.
- Will not use personal mobile phones to take photographs, video, or audio recordings of children at the service and will keep all phones etc in the staff room or office during work hours.
- Will only use educational software programs and apps that have been approved by approved provider or nominated supervisor.
- Will provide parents and families with information about the apps or software programs accessed by children at the service.
- Will ensure that appropriate websites are sourced for use with children away from children prior to use and preferably in the staff room or office.
- Will adhere to and implement the obligations under the Education and Care Services National Law and National Regulations.
- Ensure they take reasonable steps to follow the service policy and procedures and seek advice or further support if unsure.
- Ensure they complete and document any related records regarding the implementation of this policy and practice requirements of the service.
- Will attend any ongoing professional development, staff meetings and training they require to comply with this policy and practice requirements of the service.
- Will provide feedback to the nominated supervisor or approved provider regarding the policy's effectiveness, particularly in relation to identifying and responding to child safety concerns.
- Will provide feedback regarding policy review when required.

Families

- Will ensure that they are familiar with this policy and adhere to the procedures relating to the policy.
- Will refrain from taking photos within the service and at special events as the service will provide a designated staff member to record these moments.

Policy Name	**CCS- CYBER SAFETY POLICY**			Policy Version	V.2
Owner	Fishbowl Service Support Pty Ltd				
Policy published	August 2024	Last review date	August 2025	Next review date	August 2026
Service Support Within Reach	Warning -uncontrolled when printed. This document is current at the time of printing and may be subject to change without notice				

Page | 3

REGULATION IMPLEMENTATION	The following procedures outline and support all stakeholders to understand and implement the regulatory guidelines of this policy.
In regard to regulation 170- Policies and procedures to be followed.	**Approved Provider will** ▪ Ensure that all staff and volunteers are made aware of Regulatory policies and procedures by ensuring that this forms a part of the induction process. ▪ Ensure probationary reviews will be conducted once new staff are appointed at the 3- month and 6-month mark to ensure that they are following policy and procedure and to review and revise regulatory policies. ▪ Ensure staff meetings will be conducted on a regular basis to allow for review of policy and procedure and further training and revision of procedural practices in relation to policy and procedure. ▪ Ensure annual review and revision of policies and procedures will be conducted, and all educators will be given the opportunity for input.
In regard to Regulation 171- Policies and procedures to be kept available.	**Approved Provider will** ▪ Ensure that policies and procedures are available to all staff and the location and availability will form a part of the induction process. ▪ Ensure policies will be available on request for all staff members to have access when required. ▪ Ensure policies will be available when required for staff members to download copies and/or print out if required in order to complete assignments or to form part of their research and/ or update their knowledge. ▪ Ensure policies will be available for all stakeholders when requested and when updating.
In regard to Regulation 172- Notification of change to policies or procedures	**Approved Provider will** ▪ Ensure staff meetings will be conducted on a regular basis to allow for review of policy and procedure, provide further training and allow for input if required in relation to policy and procedure. ▪ Ensure stakeholders will be invited to provide feedback for policies and procedures at any time, not just on annual review but will also be invited to add feedback at review time or after an event that may require change to policy or procedure. ▪ Ensure policies and procedures will be emailed or put on display in the foyer for stakeholders to have the ability to provide feedback. ▪ Ensure feedback will be considered from stakeholders and educators and may result in a change in policy. ▪ Ensure policy and procedure may be changed at any time if there has been an incident in the service that has required a change to be implemented for the safety and health of children and or educators. ▪ Ensure in the event of a change to a policy after feedback or a situation that occurs, we will provide 14 days' notice to all stakeholders before the change takes effect
CONTINUOUS IMPROVEMENT	We are dedicated to the ongoing improvement of our practices and procedures through the following actions: ▪ Conducting regular reviews and updates of this policy with all stakeholders. ▪ Actively seeking feedback from children, families, and staff members. ▪ Providing targeted skill development and training for staff when areas for improvement are identified or when gaps in policy and procedure implementation are observed.
KEY TERMS	▪ **Approved provider**—a person who holds approval for one or more childcare services under Family Assistance Law. ▪ **Childcare software**—software developed and provided by commercial providers to interact with the Australian Government's Child Care Subsidy System (information technology system) and to support other administrative and management activities for childcare providers, personnel of services utilise this software to submit attendances, upload childcare subsidy and issue statements to stakeholders. ▪ **Proda –** is the online system where you can authenticate an individual's digital identity. ▪ **Stakeholder -** a person or group of people who have an interest in a business, a person such as an employee or customer. They have a sense of responsibility toward it and an interest in its success. ▪ **Technology-** The definition of technology is the application of scientific knowledge for practical purposes or applications. There are many different types of technology -mechanical technology, medical technology, communications technology, electronic technology, and industrial and manufacturing technologies. Though these different types of technology all serve different purposes, range in design, and are applied in different ways, they all have one thing in common:

Policy Name	**CCS- CYBER SAFETY POLICY**			Policy Version	V.2
Owner	Fishbowl Service Support Pty Ltd				
Policy published	August 2024	Last review date	August 2025	Next review date	August 2026

Service Support Within Reach   Warning -uncontrolled when printed. This document is current at the time of printing and may be subject to change without notice

Page | 4

	they all solve a problem. The word "technology" brings to mind various devices, such as laptops, phones, and tablets. Technology may also make you think of the internet, data, or advancements in the world of engineering.
WE GRATEFULLY ACKNOWLEDGE THE FOLLOWING SOURCES	▪ Australian Children's Education & Care Quality Authority. ACECQA ▪ Australian Government eSafety Commission www.esafety.gov.au ▪ Australian Government Office of the Australian Information Commissioner https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/ ▪ Code of Ethics ▪ Education and Care Services National Regulations. ▪ Education and Care Services National Law Act 2010 ▪ Earlychildhoodqld.gov.au ▪ Early Childhood Resource Hub erch.edu.au ▪ Early Childhood Australia.org.au ▪ Guide to the Education and Care Services National Law and the Education and Care Services National Regulations. ▪ Guide to the National Quality Framework. ▪ National Quality Standard. ▪ United Convention on the Rights of the Child

Policy Name	**CCS- CYBER SAFETY POLICY**			Policy Version	V.2
Owner	Fishbowl Service Support Pty Ltd				
Policy published	August 2024	Last review date	August 2025	Next review date	August 2026

Service Support Within Reach

Warning -uncontrolled when printed. This document is current at the time of printing and may be subject to change without notice

Page | 5