CHILD SAFETY & PROTECTION:

CYBER SECURITY & DATA PROTECTION

PURPOSE

This policy establishes the cybersecurity and data protection framework for our education and care service. It outlines how we protect the personal and sensitive information of children, families, educators and staff from cyber threats, data breaches and unauthorised access.

We are committed to:

- Protecting the privacy, confidentiality and integrity of all personal and sensitive information held by the service
- Maintaining secure digital systems, devices and networks
- Responding promptly and effectively to cyber incidents and data breaches
- Meeting our legal obligations under the Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme
- Aligning our practices with recognised cybersecurity frameworks, including the Australian Cyber Security Centre (ACSC) Essential Eight
- Building a culture of cybersecurity awareness among all educators and staff

---

SCOPE

This policy applies to:

- The approved provider, nominated supervisor, educators and all staff
- Students on placement and volunteers who access service systems or data
- All devices used for service purposes (whether owned by the service or personal devices used for work)
- All digital systems, platforms and applications used by the service
- All personal information held by the service, including children's records, family contact details, medical information, staff records and financial information

---

LEGISLATIVE REQUIREMENTS

This policy is informed by the following legislation, regulations and standards:

Education and Care Services National Law Act 2010

- Section 167: Protection from harm and hazards
- Section 174: Offence to fail to notify certain circumstances to the Regulatory Authority

Education and Care Services National Regulations 2011

- Regulation 168: Education and care service must have policies and procedures
- Regulation 170: Policies and procedures to be followed
- Regulation 171: Policies and procedures to be available

National Quality Standard

- Quality Area 7: Governance and Leadership
- Element 7.1.2: Management systems are in place to monitor compliance with legislation and the service's policies and procedures
- Element 7.3.5: The service builds and maintains community relationships

Privacy and Data Legislation

- Privacy Act 1988 (Cth) — Australian Privacy Principles (APPs)
- Notifiable Data Breaches (NDB) scheme — Part IIIC of the Privacy Act 1988
- Work Health and Safety Act 2011 (NSW)

Cybersecurity Framework

- Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model
- Australian Signals Directorate (ASD) guidelines for small to medium organisations

KEY DEFINITIONS

Term	Definition
Cyber Incident	Any event that compromises the confidentiality, integrity or availability of the service's information systems or data, including unauthorised access, malware infection, phishing attack or ransomware.
Data Breach	Unauthorised access to, disclosure of, or loss of personal information that could cause serious harm to an individual.
Notifiable Data Breach	A data breach that is likely to result in serious harm to one or more individuals and must be reported to the Office of the Australian Information Commissioner (OAIC) and affected individuals under the NDB scheme.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, including names, addresses, dates of birth, medical information, financial details and photos.
Sensitive Information	A subset of personal information that includes health information, racial or ethnic origin, and other categories that attract a higher level of privacy protection.
Phishing	A fraudulent attempt, usually via email, to obtain sensitive information such as passwords or financial details by impersonating a trusted entity.
Malware	Malicious software designed to disrupt, damage or gain unauthorised access to a computer system.
Two-Factor Authentication (2FA)	A security process that requires two separate forms of verification before granting access to a system or account.
ACSC Essential Eight	A baseline set of mitigation strategies recommended by the Australian Cyber Security Centre to protect organisations against cyber threats.

POLICY PROCEDURES

1. Cyber Security Standards We Follow

Our service aligns its cybersecurity practices with the Australian Cyber Security Centre (ACSC) Essential Eight Mitigation Strategies. These are:

1. Application Control — Only approved and trusted applications are installed and run on service devices.
2. Patch Applications — Software and applications are updated promptly when security patches are released.
3. Configure Microsoft Office Macro Settings — Macros are disabled or restricted to prevent malicious code execution.
4. User Application Hardening — Web browsers and applications are configured to block untrusted code.
5. Restrict Administrative Privileges — Administrative access to systems is limited to authorised personnel only.
6. Patch Operating Systems — Operating systems are kept up to date with security patches.
7. Multi-Factor Authentication (MFA) — MFA is enabled wherever possible for all systems, especially those containing personal information.
8. Regular Backups — Service data is backed up regularly and backups are stored securely and tested periodically.

2. Data Protection and Privacy

Our service will handle all personal and sensitive information in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988. We will:

- Collect only the personal information necessary for service operations
- Store personal information securely with appropriate access controls
- Ensure that personal information is not disclosed to third parties without consent, except where required by law
- Maintain accurate, up-to-date records and dispose of information securely when no longer needed
- Provide families and staff with access to their own records on request
- Have a Privacy Policy accessible to all families and staff

3. Access Control and Password Management

The following access control measures will apply to all service systems:

- Each staff member will have their own unique login credentials — shared passwords are prohibited
- Passwords must be at least 12 characters and include a mix of uppercase, lowercase, numbers and symbols
- Passwords must be changed at least every 90 days and immediately if a breach is suspected
- Multi-factor authentication (MFA) must be enabled for all cloud-based platforms and email accounts

- Access to sensitive systems and records will be granted on a need-to-know basis only
- User accounts will be deactivated immediately upon resignation or termination of a staff member
- A register of authorised users and their access levels will be maintained and reviewed at least annually

4. Device and Network Security

- All service devices (computers, tablets, smartphones) must have up-to-date antivirus and security software installed
- Operating systems and applications must be updated with the latest security patches as soon as they are available
- Personal devices used for work purposes must meet the same security standards as service-owned devices
- The service Wi-Fi network will be password-protected and use WPA2 or WPA3 encryption
- A separate guest network will be used for any visitors requiring internet access
- Staff are not to connect to public or unsecured Wi-Fi networks when accessing service systems or sensitive information
- Service devices are not to be left unattended in public places and must be locked when not in use

5. Email and Phishing Awareness

- Staff must not open suspicious emails, links or attachments from unknown senders
- Suspected phishing emails must be reported immediately to the nominated supervisor or approved provider
- The service will never request sensitive information (passwords, financial details) via email
- Staff will receive regular training on identifying phishing attempts and social engineering tactics
- Email accounts will be configured with spam filtering and, where possible, email authentication protocols (SPF, DKIM, DMARC)

6. Data Storage, Backup and Disposal

- All service data containing personal information will be stored in encrypted, password-protected systems
- Cloud storage platforms used must comply with Australian data sovereignty requirements where practicable
- A full data backup will be performed at least weekly; critical data will be backed up daily
- Backups will be stored securely, separate from the primary system (e.g., encrypted external drive or separate cloud location)
- Backup integrity will be tested at least every 6 months
- When disposing of electronic devices, all data will be securely wiped using appropriate tools before disposal or reuse

- Paper documents containing sensitive information will be shredded rather than placed in general waste

7. Staff Training and Awareness

- All educators and staff will receive cybersecurity awareness training upon commencement and at least annually thereafter
- Training will cover: identifying phishing, safe password practices, data handling, incident reporting, and use of service devices
- Records of training completion will be maintained
- The nominated supervisor is responsible for keeping up to date with emerging cyber threats and sharing relevant information with staff
- The approved provider will ensure adequate resources are allocated to maintain cybersecurity awareness across the service

8. Social Media and Online Safety

- Staff must not share photos or information about children on personal social media accounts
- Service social media accounts will have strong, unique passwords and MFA enabled
- Administrator access to service social media accounts will be limited to authorised staff only
- Any inappropriate or harmful content relating to the service or its children must be reported to the nominated supervisor immediately
- The service's Social Media Policy should be read in conjunction with this policy

CYBER INCIDENT RESPONSE PLAN

The following procedure outlines how our service will respond to a cyber incident or data breach. All staff must be familiar with these procedures.

Phase 1 — Identify and Contain (Immediate Response)

When a cyber incident is identified or suspected:

Step	Action
1	DO NOT attempt to fix the problem yourself or delete evidence. Preserve the system in its current state.
2	Disconnect the affected device from the internet and internal network immediately (unplug the Ethernet cable or disable Wi-Fi) to prevent further spread.
3	Do NOT turn off the device unless instructed by a cybersecurity professional — logs and evidence may be lost.

4	Notify the Nominated Supervisor or Approved Provider immediately, even outside business hours.
5	Document what you observed: date, time, what happened, what you were doing, any unusual messages or activity.

Phase 2 — Assess and Notify

The Nominated Supervisor or Approved Provider will:

- Assess the nature and scope of the incident — what systems or data may have been affected
- Contact an IT professional or cybersecurity specialist for technical support and investigation
- Report the incident to the Australian Cyber Security Centre (ACSC) via ReportCyber at cyber.gov.au — this is free and confidential
- Determine whether personal information has been, or is likely to have been, accessed, disclosed or lost
- If a data breach involving personal information has occurred or is suspected, immediately begin the Data Breach Assessment process (see Phase 3)
- Maintain a written Cyber Incident Log throughout the response

Phase 3 — Data Breach Response and Notification

If personal information has been, or is likely to have been, compromised:

Step 1 — Assess the Risk of Serious Harm

Consider whether the breach is likely to result in serious harm to any individual. Factors include:

- The type and sensitivity of the information (e.g., health information, financial details)
- Who may have accessed or obtained the information
- The number of people affected
- Whether the information could be used to harm the individual (identity fraud, discrimination, safety risk)

Step 2 — Notify the Office of the Australian Information Commissioner (OAIC)

If the breach is a Notifiable Data Breach (i.e., likely to result in serious harm):

- Notify the OAIC as soon as practicable, and within 30 days of becoming aware of the breach
- Use the OAIC's online Notifiable Data Breach form at oaic.gov.au
- Notification must include: description of the breach, the kinds of information involved, and recommended steps for affected individuals

Step 3 — Notify Affected Individuals

Notify all affected individuals (families, staff) as soon as practicable. Notification should include:

- A description of what happened
- The types of personal information involved
- Steps the service is taking in response
- Recommended steps the individual can take to protect themselves
- Contact details for further queries

Step 4 — Notify the Regulatory Authority (if required)

If the breach constitutes a serious incident under the Education and Care Services National Regulations (e.g., a breach affecting the safety or wellbeing of children), notify the NSW Regulatory Authority (Early Childhood Education Directorate) within 24 hours via the NQA IT System.

Phase 4 — Recovery and Review

- Restore affected systems from clean backups, verifying backup integrity before restoration
- Change all passwords and access credentials that may have been compromised
- Conduct a full security review with IT support to identify how the breach occurred and close any vulnerabilities
- Document all actions taken during the incident response
- Review and update this policy and related procedures in light of the incident
- Provide a debrief to all staff and implement any additional training identified as necessary
- Review insurance coverage, including cyber liability insurance, if applicable

EDUCATOR AND STAFF RESPONSIBILITIES

Approved Provider

- Ensure this policy is implemented and maintained across the service
- Allocate sufficient resources (financial and time) to support cybersecurity measures
- Lead or appoint a person to lead the cyber incident response
- Notify the OAIC and Regulatory Authority where required
- Ensure cyber liability insurance coverage is reviewed annually
- Review and approve updates to this policy at least every two years

Nominated Supervisor/Person in Day to Day Charge

- Be the first point of contact for any reported cyber incident
- Coordinate the service's immediate response to a cyber incident
- Ensure all staff complete cybersecurity awareness training
- Maintain the Cyber Incident Log
- Liaise with IT support and external authorities as required
- Notify the approved provider immediately upon identification of a cyber incident

All Educators and Staff:

- Follow this policy and all related cybersecurity procedures at all times
- Report any suspected cyber incidents, phishing attempts or suspicious activity immediately
- Complete all required cybersecurity training
- Use strong, unique passwords and enable MFA on all accounts
- Never share passwords or login credentials with others
- Handle personal information of children and families with care and confidentiality
- Lock devices when not in use and report lost or stolen devices immediately

RELATED POLICIES AND PROCEDURES

- Privacy and Confidentiality Policy
- Social Media Policy
- Record Keeping and Documentation Policy
- Incident, Injury, Trauma and Illness Policy
- Dealing with Infectious Diseases Policy

REFERENCES AND RESOURCES

- ACSC — Australian Cyber Security Centre: cyber.gov.au
- ACSC Essential Eight Explained: cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
- OAIC — Office of the Australian Information Commissioner: oaic.gov.au
- ReportCyber — Report a cyber incident: cyber.gov.au/report-and-recover/report
- ACECQA — Policy and Procedure Guidelines: acecqa.gov.au
- NSW Regulatory Authority — Early Childhood Education Directorate: education.nsw.gov.au/early-childhood-education

POLICY REVIEW

This policy will be reviewed at least every two years, or more frequently following:

- A cyber incident or data breach
- Changes to legislation or regulatory requirements
- Introduction of new technology systems or platforms
- Feedback from staff, families or regulatory authorities
- Significant changes to service operations

Date policy was last reviewed: 19/02/2026
Date for next review: 19/02/2028
Reviewed by: Director and Staff