Cyber Attack Policy

Policy Statement

Little Dragons Day Nursery is committed to protecting the personal information of children, parents/carers, and staff. As a nursery, we handle sensitive data every day (such as children's records, health information, and family contact details). This makes it essential that we safeguard our systems from the risk of cyber-attacks.

This policy sets out how we prevent, detect, and respond to cyber incidents to ensure the safety, security, and integrity of nursery data.

1. Scope

This policy applies to:
- All staff, volunteers, contractors, and third-party providers who use or have access to nursery IT systems.
- All devices (nursery computers, tablets, mobile phones) and online platforms (Famly, email, storage systems, etc.) used for nursery business.
- All personal data relating to children, parents/carers, and staff.

2. Objectives

- To minimise the risk of a cyber-attack disrupting nursery operations.
- To protect sensitive information from unauthorised access, misuse, loss, or damage.
- To ensure all staff understand their responsibilities for cyber security.
- To have a clear plan in place for responding to and recovering from a cyber-attack.

3. Preventative Measures

We will:
- Use secure, password-protected systems and require strong, regularly updated passwords.
- Enable multi-factor authentication (MFA) on systems where available.
- Keep all devices, apps, and operating systems updated with the latest security patches.
- Limit access to sensitive information to only those who need it for their role.
- Carry out regular backups of key data, stored securely and separately from live systems.
- Ensure staff complete cyber security awareness training, including safe email and internet use, recognising phishing, and reporting suspicious activity.
- Work with IT support and software providers to ensure compliance with recognised security standards (e.g. GDPR, ISO 27001).

4. Detection and Monitoring

- Any suspicious emails, system errors, or unusual activity must be reported immediately to the Nursery Manager, Owners and IT Support.
- IT Support will monitor systems for potential breaches or vulnerabilities.
- Regular vulnerability scans and penetration testing may be requested from providers where appropriate.

5. Response to a Cyber Attack

If a cyber-attack is suspected or confirmed, the nursery will:
1. Isolate the affected device(s) or systems to prevent further spread.
2. Report immediately to the Nursery Manager, Owners and IT Support.
3. Assess the impact – what data or systems may be compromised.

4. Notify relevant parties – including parents/carers, staff, the ICO (Information Commissioner's Office), Ofsted, or other regulators, as required.
5. Work with IT Support and providers (e.g. Famly) to contain and remove the threat.
6. Restore systems using secure backups.
7. Review and learn – identify how the attack happened, improve defences, and update training and policies.

6. Roles and Responsibilities

- Nursery Manager and Owners – overall responsibility for cyber security, policy implementation, and incident reporting.
- IT Support Provider – maintaining security measures, monitoring threats, providing technical response and recovery.
- All Staff – following safe practices, completing training, and reporting any concerns immediately.

7. Communication with Parents and Carers

In the event of a confirmed data breach or cyber-attack affecting personal information, parents and carers will be:

- Informed promptly of the nature of the incident.
- Provided with details of what information may have been affected.
- Given guidance on any steps they should take (e.g. monitoring for unusual contact).
- Updated regularly on resolution and measures taken to prevent recurrence.

8. External Software Providers: FAMLY (parent communication system) and EYWorks (staff communication system)

As our primary external software provider, Famly plays a critical role in the security of nursery data. EYWorks holds data on all of our staff team and is used as a form of communication.

We expect these systems to:

- Maintain compliance with recognised security standards and regulations (e.g. GDPR, ISO 27001).
- Ensure all data is encrypted in transit and at rest.
- Undertake regular security audits, penetration tests, and vulnerability assessments.
- Operate a clear and transparent incident response plan in the event of a cyber-attack or data breach.
- Provide prompt notification to the nursery if any incident occurs that could impact our data.
- Maintain resilient backup and recovery systems to minimise disruption in the event of an attack.
- Share updates with the nursery on ongoing improvements to their security measures.

9. Review

This policy will be:

- Reviewed annually or sooner if there is a significant change in risks or systems.

- Updated in response to new threats, technology updates, or guidance from regulators.

This policy was adopted on	Signed on behalf of the nursery	Date for review
September 2025	Kate McLeod	*September 2026*