BLACK SWAN
CYBER SECURITY SOLUTIONS

Cyber Security for Nurseries & Preschools

A Practical Guide for Early Years Providers

Why This Matters

Every day, your nursery or preschool handles deeply personal information: children's names, dates of birth, medical conditions, SEND records, staff employment details, emergency contacts, and payment information. This data is valuable to criminals and potentially harmful if exposed - making cyber security a fundamental part of your safeguarding responsibilities, not just an IT concern.

Technology now underpins nearly every aspect of early years operations. Digital systems support attendance tracking, learning observations, billing, and parent communication, but each one introduces potential vulnerabilities. According to the National Cyber Security Centre (NCSC), small organisations like nurseries are increasingly targeted precisely because criminals assume defences will be weaker. Common threats include phishing emails, malware and ransomware, often succeeding through predictable weak points: shared passwords, outdated software, or staff who haven't been trained to spot scams.

The National Day Nurseries Association (NDNA) emphasises that early years settings hold extensive sensitive and special-category data. A breach doesn't just mean lost files - it can trigger operational shutdown, reputational damage, financial penalties under UK GDPR, Ofsted concerns, and genuine safeguarding risks if children's records are compromised.

The Real-World Risk

Cyber criminals don't only target large corporations. They actively seek organisations with weak defences that can be exploited quickly, and settings using shared passwords, personal devices for work purposes, or unsecured cloud tools are particularly vulnerable.

The 2025 ransomware attack on the Kido nursery chain brought this threat into sharp focus. Personal data belonging to thousands of children and staff was stolen and published online after ransom demands went unmet. The incident generated significant media coverage and reinforced calls across the sector for improved cyber security awareness and practice.

Attackers typically use straightforward tactics: phishing emails designed to trick busy managers into revealing login credentials, or social engineering to manipulate staff into clicking malicious links. Once inside your systems, they can lock devices, steal sensitive information, or halt your operations entirely. Strong cyber security practices significantly reduce these risks and help protect both your service and your compliance standing.

Your Legal and Regulatory Obligations

As a UK nursery or preschool, you are a data controller under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. You must ensure that personal data is:

» Processed lawfully, fairly and transparently

» Collected for specified purposes and kept accurate

» Stored securely and retained only as long as necessary

» Protected against unauthorised access, loss or damage

Crucially, you must be able to demonstrate compliance - evidence matters as much as intent. The Information Commissioner's Office (ICO) provides specific guidance tailored to early years settings, including practical tips on handling children's information safely and securely.

The Early Years Foundation Stage (EYFS) statutory framework requires providers to keep records and information confidential and secure, with access restricted to those with a legitimate right or professional need to see them. This includes understanding when and how to share information appropriately for safeguarding purposes - balancing data protection with the duty to protect children from harm.

The Early Years Alliance emphasises that information sharing is essential for safeguarding, and that data protection law supports appropriate sharing when it's necessary to protect a child's welfare. The key is ensuring that sharing is proportionate, relevant, and properly documented.

While the Department for Education's Cyber Security Standards for Schools and Colleges are designed primarily for school settings, they offer valuable principles around governance, risk management, and business continuity that can inform your approach as a nursery provider.

Practical Steps to Strengthen Your Cyber Security

Effective cyber security doesn't always require technical expertise - it's built on practical, repeatable habits that your whole team can adopt:

1 Control Access Properly

Every staff member should have their own unique login credentials and use multi-factor authentication (MFA) for email and key systems. Shared passwords undermine accountability and make it impossible to track who accessed what. MFA adds a vital second layer of protection even if a password is compromised.

2 Secure All Devices

Any device used for observations, planning, or administration should be encrypted, password-protected, and set to lock automatically after a short period of inactivity. This protects data if a device is lost, stolen, or simply left unattended in a busy setting. The ICO advises that portable devices containing personal data should always be encrypted and password-protected.

All devices should also run up-to-date antivirus or anti-malware software. For Windows devices in particular, ensure Windows Defender (or equivalent commercial antivirus) is enabled and actively scanning. For settings using multiple devices or those handling particularly sensitive information, consider Endpoint Detection and Response (EDR) solutions, which provide more advanced threat detection and can identify suspicious behaviour that traditional antivirus might miss.

Apps on mobile devices (tablets and smartphones) used for nursery work should come from official app stores only, with security settings enabled and regular operating system updates applied. Avoid using personal devices for work purposes unless they're enrolled in a Mobile Device Management (MDM) system that enforces security policies.

3 Keep Everything Updated

Many successful cyber attacks exploit known vulnerabilities in outdated software. Enable automatic updates on all devices, apps, and systems -including your Wi-Fi router. This closes security gaps before criminals can exploit them.

While operating systems like Windows and macOS can update themselves automatically, third-party applications (such as Adobe Reader, web browsers, Java, and other commonly used software) often don't. These unpatched applications are frequent targets for attackers. Consider using patch management software that can automatically detect and update all installed applications across your devices. Solutions like Heimdal Patch and Asset Manager can centrally manage updates for multiple programs, ensuring nothing falls through the cracks - particularly important if you're managing several staff or child devices.

4 Back Up Regularly

Regular backups ensure you can restore essential records if data is lost, corrupted, or encrypted by ransomware. Use reputable cloud providers with data centres located in the UK or EU to support regulatory compliance, and test your backups periodically to confirm they work.

5 Train Your Team Consistently

Your staff are your first line of defence. Regular, practical training on recognising phishing emails, suspicious texts, and safe password practices makes a substantial difference. NDNA recommends short, recurring sessions with real-world examples rather than one-off generic courses. Make cyber security part of your ongoing safeguarding culture.

The ICO suggests that all staff handling personal data should understand their responsibilities, including how to store information securely, who can access it and what to do if something goes wrong.

6 Communicate Securely

When emailing parents or sharing updates via apps, ensure platforms have robust privacy protections. Remind staff never to post identifiable information about children or families on personal social media accounts, even in closed groups. Be particularly careful with photographs and videos - ensure you have proper consent and that images are stored and shared securely.

7 Vet Third-Party Providers

If you use nursery management systems, observation apps, or external IT support, scrutinise how they protect your data. Ask direct questions about encryption, multi-factor authentication, breach notification procedures, and their contractual obligations as data processors. Don’t assume compliance - verify it.

8 Establish Clear Information Sharing Protocols

Information sharing for safeguarding purposes is lawful and necessary, but it must be done correctly. The ICO’s 10-step guide to sharing information to safeguard children provides a framework for:

- Identifying when sharing is necessary and proportionate
- Recording decisions about what, when, and with whom information is shared
- Ensuring information is accurate, relevant, and not excessive
- Sharing securely using encrypted email or secure portals where possible

Understanding these principles helps you balance your duty to protect children with your obligation to protect their data.

9 Prepare for Incidents

Even strong defences can't guarantee immunity. A straightforward incident response plan should outline who to contact, how to contain a breach, when to notify the ICO (within 72 hours for reportable breaches), and how to communicate with affected families. Test this plan periodically so staff know their roles under pressure.

NDNA guidance makes clear that these foundational practices help nurseries prevent data loss, maintain parental trust, meet regulatory expectations, and ensure operational resilience.

The Safeguarding Connection

Cyber security and safeguarding are no longer separate concerns - they are deeply intertwined. Data breaches that expose children's personal information can create direct risks to their safety and wellbeing, particularly if records reveal vulnerabilities such as medical conditions, SEND support, or safeguarding flags.

The NCSC's guidance for early years practitioners explicitly connects cyber security to everyday safeguarding practice, helping settings protect both the information they hold and the systems they rely on. Keeping Children Safe in Education (KCSiE) also recognises that protecting children includes securing their data and the digital environments they interact with.

By embedding good cyber habits - secure password management, careful handling of photographs, controlled access to sensitive files etc, you not only protect data but also demonstrate your commitment to safeguarding in its fullest sense.

Further Reading

Share these official resources with your team and reference them in your policies:

NCSC – Cyber Security for Early Years Practitioners
https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings

Information Commissioner's Office (ICO) – Data Protection Tips for Early Years Settings
https://ico.org.uk/for-organisations/advice-for-small-organisations/news-blogs-and-events/blogs/data-protection-tips-for-early-years-settings/

ICO – 10-Step Guide to Sharing Information to Safeguard Children
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/

Early Years Alliance – Information Sharing
https://www.eyalliance.org.uk/advice-and-information/early-years-practice/information-sharing/

National Day Nurseries Association – Cyber Security in Nurseries
https://ndna.org.uk/cyber-security-in-nurseries/

DfE Cyber Security Standards for Schools and Colleges
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

EYFS Statutory Framework
https://www.gov.uk/government/publications/early-years-foundation-stage-framework--2

This link & version may change - Search "EYFS statutory framework" on GOV.UK for the current version

Keeping Children Safe in Education (KCSiE)
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

This link & version may change - Search "Keeping Children Safe in Education" on GOV.UK for the latest statutory guidance

Taking the Next Step

Cyber security can feel overwhelming, but it doesn't have to be. Start with one or two practical changes—enabling multi-factor authentication, scheduling automatic backups, or running a short team discussion on phishing—and build from there. Small, consistent improvements create meaningful protection and demonstrate your commitment to best practice during Ofsted inspections and regulatory reviews.

Your setting's data security is not an optional extra—it's a core part of keeping children safe, maintaining parental confidence, and meeting your legal obligations.

BLACK SWAN
CYBER SECURITY SOLUTIONS

Need Support?

Black Swan Cyber Security Solutions specialises in helping early years settings implement practical, proportionate cyber security measures that meet UK GDPR, EYFS, and Ofsted requirements. From initial risk assessments and policy development to staff training and ongoing support, we understand the unique challenges nurseries and preschools face and we're here to help you protect what matters most.

Get in touch to discuss how we can support your setting's cyber security journey.

blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142