Cyber – Nurseries and Early Years Settings

Nurseries and other early learning facilities manage large volumes of sensitive personal data, making them increasingly vulnerable to cyber-attacks.

This Loss Prevention Standard outlines the key risks and provides practical guidance to help reduce the likelihood and impact of such incidents.

Version: 1.0
Date: 11th December 2025

Cyber – Nurseries and Early Years Settings

Introduction

There are over 50,000 childcare providers in the UK. The UK Government **Childcare and Early Years Provider Survey** estimates there are over 50,000 childcare providers in the UK, employing over 360,000 members of staff. Nurseries increasingly rely on digital tools to register children, record observations, communicate with parents and manage payments. These systems often hold sensitive information, including children's names, dates of birth, health conditions, photographs, parents' addresses, emergency contact details and payment information.

In September 2025, a cybercrime group attacked a well-known nursery chain in the UK, and stole data on around eight thousand data subjects, including children and parents, published some of it on the dark web and threatened to release more unless a ransom was paid. The group behind the attack also contacted parents to pressure the nursery into paying the ransom, making national news.

This incident illustrated how vulnerable early years settings can be and how data breaches can harm children, parents, staff and the reputation of nursery chains across the UK. This document examines the unique environment in which nurseries operate, the types of data they hold, the cybersecurity risks they face, relevant laws and regulatory frameworks, and practical recommendations to strengthen cyber resilience. It draws on guidance from the National Cyber Security Centre (NCSC), UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), Early Years Foundation Stage (EYFS), Cyber Essentials certification and recent scholarly and industry sources.

Unique Characteristics of Nursery Operations and Digital Set-ups

Nurseries are often small or medium-sized enterprises (SMEs) with limited budgets for dedicated IT staff. The National Day Nurseries Association (NDNA) in an article published in September 2025 noted that "most settings are small family businesses" that do not have sophisticated IT systems. The focus is on childcare rather than technology, meaning the digital infrastructure often consists of a single office computer, a tablet or smartphone for observations, and cloud services for administrative functions such as billing, communication with parents and Finance & HR platforms.

The reliance on cloud apps can streamline administration but also increases the attack surface, especially when personal devices, insecure Wi-Fi and shared passwords are used. A hangover from the COVID-19 pandemic, many settings adopted remote working and digital platforms quickly, often without formal security assessments. Staff may be unfamiliar with basic cyber hygiene, and informal processes can persist.

Types of Data Held by Nurseries

Nurseries collect extensive personal and special-category data to comply with statutory requirements and support children's welfare. The UK GDPR requires that personal data be collected only for specific purposes, minimised, accurate and not kept longer than necessary. In practice nurseries hold:

- **Children's data:** full names, dates of birth, addresses, photos, development records, health information (medical conditions, dietary requirements), safeguarding records, learning plans and attendance logs.
- **Parents'/carers' data:** names, contact details, addresses, National Insurance numbers, payment/bank details, employment and emergency contacts.
- **Staff data:** employment records, bank details, DBS checks and safeguarding training records.
- **Operational data:** CCTV footage, visitor logs, accident forms and communications with external agencies (social services, Ofsted, local authorities).

The sensitivity of this data means that a breach can expose children to identity theft, grooming or safeguarding risks. Presently under the UK GDPR, nurseries act as data controllers for the information they collect and must implement appropriate technical and organisational measures. They also often share data with third-party processors such as childcare platforms or payment providers and therefore must conduct due diligence and data processing agreements.

Regulatory framework and legal obligations

UK nurseries must comply with legal and regulatory requirements including (but not limited to):

1. **UK GDPR**. The UK GDPR principles require personal data to be processed lawfully, transparently, for specific purposes, be adequate, relevant and limited, accurate, retained only as long as necessary, and handled securely. Providers must also be accountable, able to demonstrate compliance through policies, staff training and documentation. Some requirements within the nursery setting may include:
    - Providing clear privacy notices to parents explaining data use, lawful bases and retention periods.
    - Obtaining valid consent where necessary (e.g., use of photos on websites), ensuring it is explicit and not pre-ticked.
    - Honouring data subjects' rights (access, rectification, erasure, portability and objection).
    - Maintaining records of processing activities and conducting Data Protection Impact Assessments (DPIAs) for high-risk processing (e.g., CCTV or new digital platforms).
    - Reporting serious data breaches to the Information Commissioner's Office (ICO) within 72 hours and informing individuals if there is a high risk to their rights.

2. **Early Years Foundation Stage (EYFS) and safeguarding**. The EYFS statutory framework requires confidential information about children to be securely maintained and accessible only to those who have a professional need. The full wording from section 3.93 of the Early Years Foundation Stage statutory framework or group and school-based providers notes:

   "Records must be easily accessible and available (these may be kept securely off the premises). Confidential information and records about staff and children must be held securely and only accessible and available to those who have a right or professional need to see them59. Providers must be aware of their responsibilities under the Data Protection legislation56 and, where relevant, the Freedom of Information Act 2000."

   Early years services must ensure staff understand the need to protect privacy and handle information confidentially. The NCSC emphasises that good cybersecurity is part of safeguarding.

3. **Health and Safety and Employment law**. Nurseries must comply with health and safety regulations and maintain secure records such as accident forms, risk assessments and staff employment information. Data breaches of this nature could expose early years settings to legal liabilities.

Cyber Threat Landscape for Nurseries

- **Ransomware and Extortion.** In the attack described earlier on, hackers stole and published personal data of children, then demanded a ransom from the nursery and contacted parents. Ransomware gangs often target SMEs because their defences may be less sophisticated than larger organisations and they have been known to pay quickly to resume operations. The stolen data can be sold for identity fraud, phishing or blackmail. Many early years settings have not tested backups or incident response plans, increasing downtime and potential regulatory fines.
- **Phishing and Social Engineering.** Phishing attacks are a primary method for initial access. The NCSC's early years guidance warns that scammers send emails or texts that appear to be from trusted organisations (e.g., HMRC, Ofsted, parcel companies) and try to trick recipients into disclosing passwords or clicking malicious links. Indicators include urgent requests, official looking links, attachments or offers of compensation. Staff may also receive fraudulent invoices or requests to change bank details. Attackers exploit the goodwill and busy schedules of nursery staff. In the incident referenced above, criminals called parents, impersonating the nursery and urging them to apply pressure to the company.
- **Insider Threats and Human Error**. Accidental data breaches can occur when staff email personal data to the wrong recipient, lose USB drives, or misconfigured cloud storage. Use of personal devices without strong passwords or antivirus software can lead to malware infections. Staff may share logins to save time, preventing accountability and increasing the risk of misuse. High staff turnover means training must be repeated regularly.
- **Supply-Chain Risks**. Nurseries often rely on third-party IT providers, payroll companies, and educational platforms. A breach at a third-party provider could expose their data. GDPR requires nurseries to ensure processors provide sufficient guarantees and to have contracts regulating data use.

- **Physical Threats**. Paper records and devices can be stolen or accessed without permission. Nurseries must lock filing cabinets and restrict access to offices. Loss of laptops or tablets containing unencrypted data can lead to significant breaches. The EYFS emphasises physical security alongside digital security.

Risk Management and Governance

- **Establishing a Security Culture**. A strong security culture relies on leadership commitment and staff awareness. Management should create policies that set expectations for data handling, internet use, remote working and incident reporting. The accountability principle of GDPR requires that staff receive training and understand their obligations. Ongoing training should cover recognising phishing, creating strong passwords, handling confidential information, and reporting suspicious activity. The National Day Nurseries association emphasises that nurseries must be particularly vigilant because of the data they hold.
- **Conducting Risk Assessments and Data Protection Impact Assessments (DPIAs)**. Risk Assessments and DPIAs should be documented, understood and reviewed annually or when significant changes occur.

  A cyber risk assessment identifies critical data assets, threats, vulnerabilities and the likelihood and impact of incidents. It should examine hardware, software, networks, cloud services, third-party providers and physical security.

  DPIAs are used for new technologies, such as CCTV or digital learning apps, to assess privacy risks and implement mitigating measures (e.g., encryption, pseudonymisation). Consideration should be given to (data availability), phishing (confidentiality), and insider error.
- **Data Minimisation and Retention**. Under the UK GDPR, personal data should be adequate, relevant and not excessive. For example, do not store unnecessary copies of birth certificates or medical records. Implement retention schedules to delete or anonymise data when children leave the setting or statutory periods expire. Many nurseries keep data longer than necessary due to habit or fear of inspections. A clear retention policy reduces the amount of data at risk during a breach.
- **Third-Party Management**. Ensure contracts with software providers (e.g., parent communication apps, payroll services) include data protection clauses, specify processing instructions and require incident notification. Consider access controls when using these services, and if the option to enforce multi-factor authentication exists, it should be implemented. Assess their security certifications and ask whether they meet standards like ISO 27001 or Cyber Essentials. Confirm their data storage locations (UK/EU), encryption practices and backup strategies. Under GDPR, controllers remain responsible for data protection even when using processors.
- **Incident Response and Reporting**. Develop a plan that outlines steps to take when a breach occurs: identify and contain the incident, preserve evidence, assess the scope, notify management and data protection officer (if appointed), contact the IT provider, details on insurance policies and consider disconnecting affected devices.

  The plan should include communication templates for informing parents and employees and a contact list for authorities (Information Commissioners Office, police, NCSC).

Serious breaches must be reported to the ICO within 72 hours. Simulating events and attacks through tabletop exercises is always recommended and help staff to respond appropriately, comprehensively and calmly during real events.

Technical Controls and the Cyber Essentials Certification Scheme

There are several baseline controls that should be in place across every single organisation in the UK. They span different areas, and a useful starting point for a lot of businesses in the UK is the Cyber Essentials Certification scheme, administered by IASME.

Overview of the Cyber Essentials Certification Scheme

Cyber Essentials is a UK Government-backed scheme that aims to help organisations of all sizes implement basic cyber hygiene. Cyber Essentials' five controls have been touted to reduce up to 80 percent of common attacks. These controls align well with nursery and early-years operations because they are simple, cost-effective and address key vulnerabilities.

1. **Firewalls and Boundary Security**. Firewalls should be configured to only allow traffic necessary for operations and should block unauthorised access. For nurseries, this means ensuring broadband routers and Wi-Fi routers have secure administration passwords, disabling remote management unless needed, and regularly updating firmware. Guest Wi-Fi networks should be separate from networks used for business devices. Use network-level blocking to restrict access to harmful websites.
2. **Secure Configuration**. Devices should be configured to reduce vulnerabilities: remove unused accounts, disable unnecessary services, change default passwords and restrict physical ports. For example, a new laptop should not use an open administrator account; create standard user accounts for staff and restrict installation rights. Uninstall pre-installed apps that are not required. Enable disk encryption (e.g. BitLocker on windows devices) and automatic screen lock after a short period of inactivity. The Center for Internet Security has an extensive library of "hardened" images that are more secure versions of common operating systems, such as MacOS and Windows. It can be found here.
3. **Security Update Management**. Keep operating systems, applications and firmware up to date with the latest patches to avoid known vulnerabilities. Enable automatic updates for Windows, iOS, Android and third-party software. Replace unsupported devices and software (e.g., Windows 7) to maintain security. Maintain an asset register to track devices and their update status.
4. **User Access Control**. Grant staff only the access they need to perform their role and restrict administrator privileges to trusted individuals. If there are administrative accounts in the environment, they should not be used for day-to-day activities, and they should separate from user accounts. Each member of staff should have a unique login and password combination and should not share accounts. Enforce the use of multi-factor authentication on sensitive systems such as email, cloud platforms and parental communication apps. Remove access promptly when employees leave or change roles. For volunteers or students on placements, provide limited guest accounts.

5. **Malware Protection**. Install reputable antivirus or anti-malware software on all devices and ensure it updates automatically. Where possible, use application whitelisting and built-in protections such as Windows Defender. Educate staff not to download apps from unofficial sources or click suspicious links . Consider using mobile device management (MDM) solutions to enforce security policies on tablets and smartphones.

NCSC Early Years Cyber Security Guidance

The NCSC produced specific guidance for early years practitioners, summarised by the Government and industry blogs. It emphasises four key actions:

1. **Back Up Important Information**. identify critical information (children's records, payroll, financial data) and back it up regularly on a USB, external hard drive or a secure cloud service. Keep backups disconnected from the network to avoid ransomware infection and test restoration procedures (i.e., ensure it is clear how the backups can be restored). Encrypt backups and store them in a locked cabinet or safe.
2. **Use Passwords to Control Access.** Protect all devices (computers, tablets, phones) with passwords or PINs; set devices to lock automatically; create strong passwords using three random words and avoid reusing passwords across accounts. Do not repeat email or application passwords across multiple interfaces. Use password managers and enable multi-factor authentication on critical accounts.
3. **Protect Devices from Viruses and Malware.** Ensure antivirus software is installed and updated; apply software updates promptly; and only download apps from official app stores . Use parental control or mobile device management to restrict downloads on tablets used with children.
4. **Deal with Suspicious Messages**. Teach staff to recognise phishing emails or texts (look for spelling errors, urgent requests, mismatched URLs); verify unusual requests by contacting the sender through known channels; do not click links or open attachments; and report suspicious emails to the NCSC's phishing reporting service. The guidance emphasises that early year's providers must train staff to challenge unusual requests and never reveal passwords or bank details over email. If a staff member accidentally responds to a phishing email, change the password immediately and report the incident.

Practical Recommendations for Nurseries

For Nursery Owners and Management

1. **Appoint a Data Protection Lead**. While the GDPR requires a Data Protection Officer only for public authorities or organisations processing large amounts of special-category data, having a designated person who understands data protection and cyber security enhances accountability and ultimately helps to make your business safer. This individual should oversee privacy policies, DPIAs, staff training and breach response processes.

2. **Obtain Cyber Essentials Certification.** Pursue Cyber Essentials and potentially Cyber Essentials Plus certification to demonstrate baseline security practices. Certification provides a structured approach and may reduce the likelihood of being the victim of a cyber-attack. Many local authorities encourage early years settings to adopt Cyber Essentials.
3. **Document Policies and Procedures.** Maintain written policies for data protection, acceptable use, password management, portable devices, remote working and incident response. Ensure policies align with GDPR and EYFS guidance and are communicated to staff and parents.
4. **Engage with IT Professionals and Insurers.** If internal expertise is limited, partner with a reputable IT support company to implement security controls, monitor systems and provide technical incident response. Consult insurance brokers to understand coverage for ransomware, data breaches and regulatory fines. Insurers often ask about controls that are found within Cyber Essentials certification scheme.
5. **Budget for Cyber Security.** Allocate resources for secure devices, software licences, training and periodic audits. Consider the cost of a potential breach which includes ICO fines, legal fees, lost business and reputational damage. Compare this with preventative investment.
6. **Plan for Continuity.** Consider the development and testing of business continuity and disaster recovery plans, including manual processes for operating without IT systems. Ensure cash flow is available to restore operations after a breach or extended outage.

For Nursery Staff and Practitioners

1. **Follow Security Policies.** Use unique passwords; avoid sharing logins; lock computers when away; and store paper records securely. Immediately report lost devices, suspected phishing messages or unusual system behaviour.
2. **Be Cautious with Emails and Texts.** Verify the sender's identity, especially when being asked to transfer money or provide sensitive information. Use the official telephone number rather than details in the email. Report suspicious messages to management and the NCSC .
3. **Use Secure Communication with Parents.** When sending messages or photos of children, use secure parent-portal apps rather than personal email or messaging apps. Ensure privacy settings are configured and avoid sharing children's data on social media without explicit consent.
4. **Protect Devices Used with Children.** Keep tablets and cameras used for observations separate from personal devices; ensure they have passcodes, encryption and antivirus software. Avoid storing photos on personal phones.
5. **Stay Updated.** Attend provided training on cyber security, data protection and safeguarding. Learn how to identify new scams and apply security updates.

Conclusion

Nurseries and other early years settings are attractive targets for cyber criminals due to the sensitive information they hold, and the increased likelihood that cybersecurity resources will be scarcer. Attacks on the industry are shocking to many people outside of the cybersecurity community, whilst it confirmed a well held truth that many inside the industry believe:

- No business or sector is off limits for cyber criminals.

Nurseries must comply with UK GDPR and EYFS requirements to ensure confidentiality, integrity and availability of data. By adopting a defence in depth approach of combining governance, staff training, robust policies, technical controls (such as those in Cyber Essentials) and swift incident response procedures, nurseries can significantly reduce the risk of suffering a successful cyber-attack.

Investment in cyber security is not just a technical issue. It is integral to safeguarding children and maintaining the trust of parents, staff and regulators.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

- Cyber Security Awareness Training - **Phishing Tackle**
- Business Continuity, crisis communications - Horizonscan

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- Malware Bytes article Hackers Threaten Parents: Get Nursery to Pay Ransom or we Leak Your Childs Data
- NDNA article NDNA Response to the Kido Nurseries Cyber Attack
- West Northamptonshire Council GDPR Guidance for Childcare Providers
- Early Years Alliance Information Sharing and Data Protection https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings
- IT Governance article The 5 Cost-Effective Security Controls Everyone Needs
- NCSC guidance document Cyber Essentials: Requirements for IT Infrastructure v3.2
- Gov.UK Childcare and Early Years Provider Survey 2024
- BBC News article Children's names, pictures and addresses stolen in nursery chain hack

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

Relevant Aviva Loss Prevention Standards include:

- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks**
- **Cyber Security: Respond and Recover**
- **Cyber Security: The Internet of Things**
- **Ransomware - Cyber Loss Prevention Standard**
- **Cyber Essentials - Accreditation**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

11th December 2025

Version 1.0

ARMSGI3582025

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.