NURSERY CYBER SECURITY CHECKLIST

BLACK SWAN
CYBER SECURITY SOLUTIONS

Practical steps for nurseries, preschools & after school clubs

Why this checklist matters

Nurseries, preschools and out-of-school clubs hold some of the most sensitive information in education - children's records, safeguarding notes, parent communications and payment details.

Ofsted, **KCSIE, EYFS** and **GDPR** all expect providers to protect this data with the same care given to physical safeguarding.

Recent attacks on early years organisations, including the Kido International breach, show how vulnerable even well-run settings can be.

This checklist helps you identify gaps, strengthen digital safeguarding and demonstrate compliance during inspections or trustee meetings.

1 Safeguarding & leadership responsibilities

- [ ] A named DSL (and deputy) understands how cyber risks affect safeguarding.
- [ ] Leaders know their obligations under **KCSIE, Ofsted, EYFS** and **GDPR**.
- [ ] A clear process exists for reporting suspicious emails, texts or parent-messages.
- [ ] Staff know who to contact immediately if something "looks wrong."

2 Secure devices (laptops, tablets, shared PCs)

- [ ] All staff devices have up-to-date antivirus/EDR.
- [ ] Shared tablets are locked down with passcodes or MDM controls.
- [ ] Devices auto-update and install security patches promptly.
- [ ] USB ports are restricted on shared machines (where possible).
- [ ] Staff have unique logins – no shared passwords.

3 Protecting children's data

- [ ] Digital safeguarding notes are stored securely and access is restricted.
- [ ] EYFS observations (Tapestry, Famly, EYLog, Blossom) use strong passwords.
- [ ] Staff do not store children's data on personal devices.
- [ ] Records are backed up offsite or in the cloud.
- [ ] Backups are tested regularly to ensure they can be restored.

4 Strong email & account security

- [ ] Multi-factor authentication (MFA) is enabled on all staff accounts.
- [ ] Staff can spot fake-parent messages, invoice scams and phishing.
- [ ] Email security tools protect against impersonation and malicious links.
- [ ] Passwords are unique and not reused.
- [ ] Accounts are disabled promptly when staff leave.

5 Safe browsing & DNS filtering

- [ ] DNS filtering blocks harmful or inappropriate websites.
- [ ] No devices connect to unsecured public Wi-Fi.
- [ ] Ad-blocking is enabled to reduce malicious advert risks.

6 Parent communication & payment systems

- [ ] Parent-apps (Tapestry, Famly, ParentMail, EYLog, Blossom) follow secure login policies.
- [ ] Billing and payment systems use strong passwords and MFA.
- [ ] Staff verify changes to bank details by phone, not email.
- [ ] Only authorised staff access billing and attendance systems.

7 Backup, recovery & business continuity

- [ ] All critical data is backed up daily.
- [ ] Backups are stored offsite or in secure cloud storage.
- [ ] Recovery processes are tested quarterly.
- [ ] The nursery has a simple written incident plan staff know how to follow.

8 Staff training & awareness

- [ ] All staff receive short, practical cyber-safety refreshers (termly).
- [ ] DSLs understand digital safeguarding risks.
- [ ] New starters receive cyber awareness as part of induction.
- [ ] Regular reminders cover safe passwords, data handling and reporting concerns.

9 Visitor, contractor & supply chain risks

- [ ] Only trusted contractors access the nursery's network or systems.
- [ ] No unmanaged or borrowed devices connect to staff Wi-Fi.
- [ ] External childcare software is checked for security reputation.

10 Policies, documentation & evidence

- [ ] Clear policies exist for data protection, acceptable use, mobile devices, photos, digital media and incident reporting.
- [ ] Leaders can show evidence of device protection, access controls, regular backups, staff training and risk assessments.
- [ ] Trustees or owners receive simple security updates each term.

11 Physical security

- [ ] Staff devices are locked away when not in use.
- [ ] Screens lock automatically after a short period.
- [ ] Visitors cannot view staff screens containing children's data.
- [ ] CCTV systems are password-protected and securely maintained.

BLACK SWAN
CYBER SECURITY SOLUTIONS

Want support?

If you're unsure where to start or want reassurance that your nursery's digital safeguarding meets Ofsted and GDPR expectations, we can help.

Black Swan Cyber Security Solutions specialises in affordable protection for early-years settings - keeping data, devices and parent systems safe.

blackswancyber.co.uk

hello@blackswancyber.co.uk

01246 927142