kinderpedia

A practical cybersecurity guide for schools and nurseries

10 essential measures you can start implementing tomorrow



Developed by Kinderpedia,
in collaboration with Black Bullet

BLACK BULLET
ON TARGET DIGITAL SOLUTIONS



Why this checklist matters

Modern education relies on connection: school leaders, teachers, and parents communicate online, utilize digital tools, share photos, and access sensitive information about children.

At the same time, cyber-attacks are becoming increasingly creative, ranging from phishing emails and fake messages to unauthorized access to WiFi networks or surveillance systems.

For schools and nurseries, digital security is no longer a “nice to have”. It is a critical responsibility linked to safeguarding personal data, protecting your community, and maintaining parents’ trust in your institution.

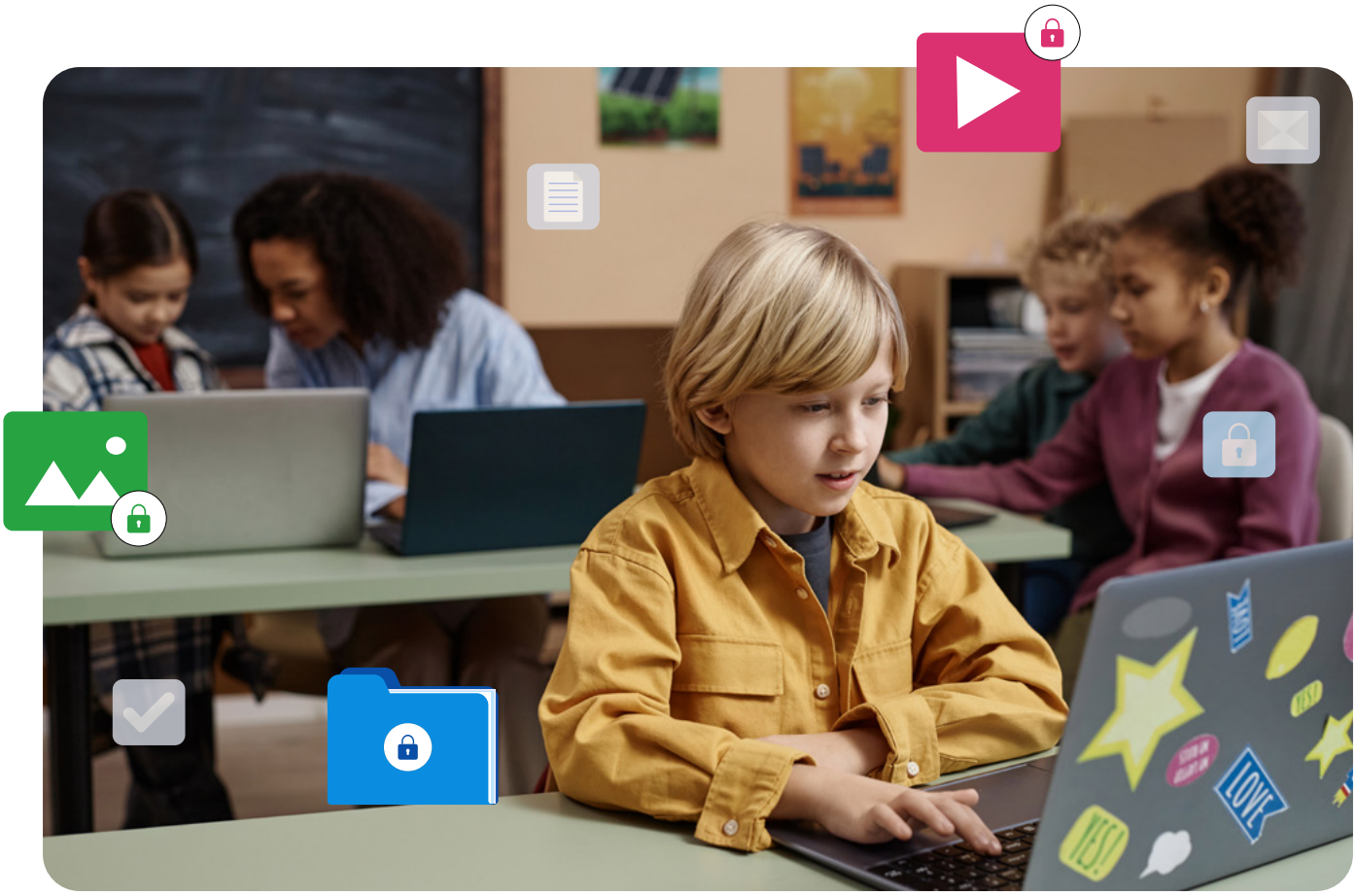


This checklist helps you:

- identify real risks,
- put simple, effective measures in place,
- strengthen your school’s digital resilience,
- stay compliant with GDPR requirements.

And the best part?
You don’t need a large IT department to get started.





10 essential cybersecurity measures for schools & nurseries

1 Use strong passwords and a password manager

Every account in your school should have a complex, unique password (e.g: CrtuFtsq*93c!). A **password manager** makes this simple: it saves you time and dramatically reduces risks.

2 Enable two-factor authentication (2FA/MFA)

A password alone is no longer enough. Add an extra code for email accounts, platforms, CCTV systems, administrative access, and digital registers

3 Keep all systems updated

Updates come with protection. Enable automatic updates for devices, apps, routers, and surveillance systems.

4 Back up your data and test recovery regularly

A backup is useful only if you can restore it. Test the recovery process monthly, so you know it works when you need it most.

5 Limit access: each person sees only what they truly need

Apply the “least privilege principle”. Review permissions at the start of every term and whenever someone leaves the institution.

6 Secure your school network (especially WiFi)

- Separate WiFi for visitors
- Unique passwords, not factory defaults
- WPA3 encryption
- Network segmentation: visitors/ staff /admin

7 Run short, regular training sessions for staff

They don’t need to be technical. **5–10 minutes a month** on:

- phishing
- suspicious links
- fake QR codes
- unsafe attachments

8 Check and secure all connected devices

Any device brought into school (phone, laptop, tablet) should have up-to-date antivirus protection and system updates installed.



9 Create and test an incident response plan

Your school should know:

- who acts first,
- how staff and parents are informed,
- what happens to compromised accounts,
- when and how to notify the Data Protection Authority.

10 Carry out regular security audits

An external audit once a year (or every six months) helps you discover vulnerabilities before attackers do.

5 GDPR principles every school & nursery must follow



1 **Collect only the data you genuinely need**

Avoid gathering information “just in case”.

2 **Clearly explain to parents why you collect data**

This applies to CCTV, apps, enrolment, registers, communication tools, and more.

3 **Use audited and certified platforms**

Kinderpedia undergoes regular security audits and penetration tests with Cyberwall and is certified under **ISO 9001:2015** and **ISO/IEC 27001:2022**. This confirms high-quality processes and rigorous protection of personal data.

4 **Be mindful of the images you publish online**

Promotion is important, but children’s photos must be handled responsibly.

5 **Review all internal data protection policies annually**

Compliance is not a document — it’s an ongoing process.

3 things you can implement as early as tomorrow

Enable 2FA for all administrative and leadership accounts.





Set up a separate WiFi network for visitors and personal devices.

Change the default passwords on cameras and routers.





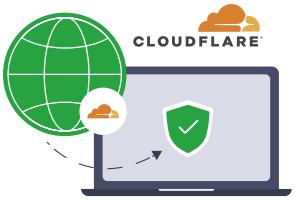
How does Kinderpedia protect your entire school community every single day?

Cloud hosting on AWS



Kinderpedia is hosted on Amazon Web Services (AWS), in secure European data centres located in Frankfurt, Germany. This ensures full alignment with EU data protection legislation (GDPR). The platform uses dedicated AWS services such as Amazon EC2, RDS, and Elastic Load Balancing that ensure stability and security. All databases and files benefit from **daily backups** and **redundancy**, guaranteeing availability and data integrity.

Advanced perimeter protection via Cloudflare



Kinderpedia uses Cloudflare to protect the platform against distributed attacks (DDoS), malicious traffic, and attempts to exploit vulnerabilities. Cloudflare filters and blocks suspicious requests before they reach our servers and accelerates content delivery for a faster, safer user experience.



Micro-services architecture with fragmented data

Kinderpedia is built on a micro-services architecture that separates data both logically and physically. In the extremely unlikely event that a single server would be compromised, the attacker would only access **isolated, partial, unusable data fragments**. Information is stored and processed in small, independent components, reducing the risk of an integral data breach and increasing platform resilience.



Regular cybersecurity audits and pen-tests

Kinderpedia conducts periodic cybersecurity audits and penetration tests in partnership with **Cyberwall**, a company authorised by the **European Cybersecurity Competence Centre**. These assessments confirm that the platform passes rigorous penetration, security, and resilience tests across both web and mobile apps (Android and iOS).



International quality and security certifications

Kinderpedia is certified according to **ISO 9001:201**5 and **ISO/IEC 27001:2022**, two internationally recognised standards.

- ISO 9001 ensures consistent processes and high-quality services.
- ISO/IEC 27001 confirms that Kinderpedia implements strict information security controls aligned with the most advanced industry practices.



Daily backups and continuous maintenance

Daily backups are performed automatically for all critical systems and data. Security patches, updates, and maintenance are included in the standard service contract at no additional cost for institutions.



Full data confidentiality and ownership

All data and documents uploaded by schools remain **the exclusive property of the institution**. Kinderpedia acts as a GDPR-compliant **data processor**, ensuring confidentiality and enabling full data portability toward external systems (e.g., SIIIR, BRIO).

Granular user access and the principle of least privilege

Institution administrators can configure precise access levels for each user role. Kinderpedia applies the least-privilege principle. This ensures that every user only accesses the information strictly necessary for their responsibilities, reduces exposure, and limits potential impact in case of a compromised account.

Complete audit log for access changes

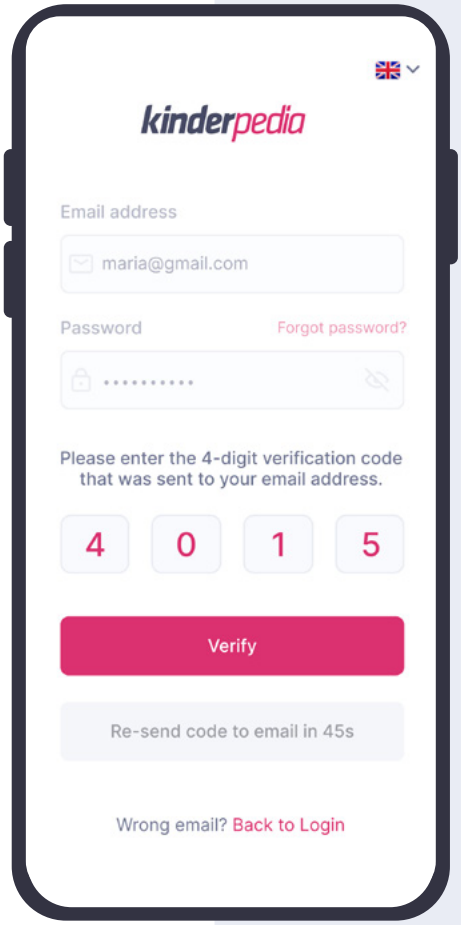
Kinderpedia includes an in-depth Audit Log that records every change made to user permissions or access rights. This guarantees transparency, accountability, and full traceability across the platform.

Two-factor authentication (2FA) and OTP codes

Each user has a unique password and can enable two-factor authentication. Upon login, the system sends a one-time password (OTP) to the user's email, adding an extra layer of protection against unauthorised access.

Device management & "log out of all devices"

Kinderpedia provides a dedicated Device Management panel where users can see all active sessions and connected devices in real-time. Suspicious devices can be disconnected instantly, while the "Log Out of All Devices" option allows immediate, simultaneous logout from all terminals. This ensures a rapid response in case of security concerns.



kinderpedia

We build modern education with genuine care for your data.

Digital security is no longer a technical afterthought; it is part of the culture of a resilient school. With simple, consistent measures, you can protect the data of children, teachers, and parents, while maintaining efficiency and strengthening trust in your community.

Would you like to see how Kinderpedia can help you create a safer digital environment?

Book a conversation with our team

