

School Guest Wi-Fi Checklist

A practical guide to secure, simple visitor access for schools and MATs



Use this checklist to review whether your guest Wi-Fi keeps visitors separate, protects school data and remains easy for staff to manage.

Secure. Simple. Smart.
Wi-Fi that works for your school.

Guest Wi-Fi Security Checklist

Tick each item that is already in place. Anything left unticked should be reviewed as part of your next Wi-Fi health check, network audit or school infrastructure refresh.

☐	Separate guest network Visitors connect to a dedicated guest network that is isolated from staff, student, admin and curriculum systems.
☐	Individual authentication Access is issued per visitor, group or event rather than relying on one shared password that is rarely changed.
☐	Time-limited access Guest access expires automatically after a set period, such as the end of the school day, meeting or contractor visit.
☐	Internet-only access Guest users can reach the internet but cannot access servers, printers, safeguarding systems, finance platforms or internal devices.
☐	Logging and visibility The school can see who connected, when they connected and which access method was used, in line with policy requirements.
☐	Cloud management The guest network can be managed centrally, making changes quicker across one school or a multi-academy trust.
☐	Bandwidth controls Guest traffic is limited or prioritised so visitor devices cannot affect lessons, exams, cloud applications or staff systems.
☐	Clear acceptable use policy Visitors are shown a simple usage notice or captive portal before they connect.
☐	GDPR and safeguarding considerations Guest access is designed with data protection, safeguarding and accountability in mind.
☐	Regular review Guest Wi-Fi settings, passwords, portals and policies are reviewed regularly, not left unchanged for years.

Quick rule: guest Wi-Fi should be easy for visitors to use, but difficult for the wrong people to abuse.

Score Your Current Guest Wi-Fi Setup

Add up the number of checklist items you can confidently tick.

0-3	High risk Your guest access may be creating unnecessary security, safeguarding or performance risks. Prioritise a review.
4-7	Needs improvement Some good controls may be in place, but gaps remain. Focus on isolation, visibility and access expiry.
8-10	Good foundation You have a strong base. Review regularly and confirm that the setup still matches current users, devices and policies.

Common Warning Signs

- ! The same guest password has been used for months or years.
- ! Reception or office staff manually share passwords with no expiry date.
- ! Visitors can see printers, shared drives, classroom devices or internal systems.
- ! There is no simple record of who was connected and when.
- ! Guest devices slow down lessons, exams, video calls or cloud platforms.
- ! Each school in a MAT manages guest access differently with no central standard.

Your Next Steps

Use the boxes below to turn the checklist into a practical action plan for your school or trust.

Priority area	Action needed	Owner / date
1.		
2.		
3.		
4.		
5.		

Not sure if your school guest Wi-Fi is secure?

Book a free Wi-Fi Health Check with Redway Networks. We can review your current guest access, identify security and performance risks, and recommend practical improvements for your school or MAT.

redwaynetworks.com | 01908 046 400

Redway Networks specialises in the planning, design, configuration and installation of enterprise-grade Wi-Fi and networking solutions for schools and businesses. Our projects are delivered by certified, experienced network engineers.