Department for Education

Title:	**Wireless Network Standards**
Published:	23 March 2022
Updated:	-

Find out what standards your school or college should meet on wireless network performance, coverage, management and security.

#	Standard	Page
1	Use the latest wireless network standard approved by the Wi-Fi Alliance	2
2	Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required	3
3	Have a solution that can centrally manage the wireless network	4
4	Install security features to stop unauthorised access	5

Standard 1

Use the latest wireless network standard approved by the Wi-Fi Alliance

The importance of meeting the standard

Your school or college will have a high number of users accessing the network at the same time. A high-performance solution is needed to make sure that the speed of the connection does not slow down as more devices connect to the wireless network.

How to meet the standard

You should ask your supplier or in-house support team to provide a wireless solution that uses the Wi-Fi 6 standard.

Technical requirements to meet the standard

The wireless network should use the latest standard approved by the Wi-Fi Alliance, Wi-Fi 6 (802.11ax). You should also review the network interface speeds of the access points when considering the solution – these will typically be 1Gbps, 2.5Gbps and 5Gbps.

The wireless network should be configured to support network segregation and QoS.

Dependencies to the standard

The speed of your wireless connection may be affected by your internal network cabling and switches.

See other standards on network cabling and switches.

When to meet the standard

You should meet the standard when you need to upgrade an underperforming or unsupported solution.

Standard 2

Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required

The importance of meeting the standard

Like with mobile phones, a good wireless connection relies on signal strength. It's important to make sure there is strong signal coverage in all areas of your school or college where mobile devices are to be used.

How to meet the standard

You should have wireless access points installed across the site. This could be up to one per classroom.

Technical requirements to meet the standard

Ensure that the number of access points provides coverage in each space that is in line with the planned occupation level. This is to support simultaneous use without reducing the performance.

You should ensure that your wireless provider designs a solution that fully meets your needs. This should include using wireless heat mapping as part of initial planning and ensuring that impact from building management systems and other networks is minimised.

Dependencies to the standard

The speed of your wireless connection may be affected by your internal network cabling and switches.

See other standards on network cabling and switches.

When to meet the standard

You should meet the standard when you need to upgrade an underperforming or unsupported solution.

Standard 3

Have a solution that can centrally manage the wireless network

The importance of meeting the standard

A wireless network will be made up of many wireless access points. A central management solution will allow your support team to monitor and configure your network and identify and resolve issues.

How to meet the standard

Your wireless network provider or in-house support team should provide a central management tool that can be used to configure the wireless access points, monitor performance and provide alerts in the event of a failure.

It should also have the functionality to deliver software security updates automatically as soon as they are available. Manual checks should also be undertaken.

Technical requirements to meet the standard

You should ask your supplier to make sure that the wireless solution will:

- provide active signal management and load balancing of user or device connectivity
- have tools that can be used to configure the wireless access points, monitor performance and provide alerts in the event of a failure
- include a manufacturer warranty and support arrangements including licences, software enhancements and firmware updates
- include an on-site, system administrator training package, that is manufacturer approved and that covers all security elements for the solution
- be scalable and can accommodate future higher bandwidth requirements
- be capable of providing a configuration file that allows the solution to be reset to the original configuration for the school

When to meet the standard

You should meet the standard when you need to upgrade an underperforming or unsupported solution.

Standard 4

Install security features to stop unauthorised access

The importance of meeting the standard

Your school or college IT networks should prevent access by unauthorised users while providing access to regular and guest users.

A wireless network without adequate security may allow unauthorised users access to secure information stored by the school or college. This could lead to:

- theft or misuse of sensitive school or student data
- loss of access to critical school systems
- significant disruption and cost

How to meet the standard

Ask your wireless network provider, supplier or in-house support team for a proposal that will support the latest Wi-Fi Alliance specification mentioned in technical requirements to meet that standard.

The solution should also ensure that users must not be able to access the network without appropriate authorisation and authentication methods. Any administrative accounts that have access to make configuration changes, must be secure and fully documented.

Technical requirements to meet the standard

The network solution should ensure that authorised mobile user devices or guest users are securely authenticated individually onto the network. The network traffic should be protected from external and unauthorised internal interception while not impacting on the network's performance.

To achieve this, you may need:

- virtual local area networks (VLANs)
- access control lists (ACLs)
- secure segregated guest access
- the latest authentication protocols (WPA3)
- wireless intrusion protection (WIPs)
- certificate-based authentication
- multi-factor authentication (MFA) for privileged users and technical support staff

When to meet the standard

You should meet the standard when you need to upgrade an underperforming or unsupported solution, or following a scheduled maintenance or configuration review.