

# Bring Your Own Device FOR SCHOOLS

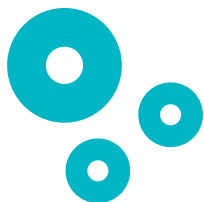


Technical advice for  
school leaders and  
IT administrators

# Contents



Related guides, booklets and on-line resources that you may find helpful: .....	3
What do we mean by BYOD?.....	4
Factors that affect BYOD technical requirements and options .....	4
Will our technical infrastructure support BYOD? .....	5
Common technical challenges for schools implementing BYOD .....	5
Keeping up with developing requirements .....	6
Connectivity and obtaining the necessary broadband speed .....	6
Wi-Fi coverage and capacity .....	6
Device management .....	7
Control of access via BYOD devices to educational and other content .....	7
Access to electricity supply .....	7
Safeguarding students from potential on-line risks .....	7
Acquiring devices to be used for BYOD .....	7
Switching to, or increasing the use of, web based learning materials .....	8
Mismatch between students and teachers expectations and knowledge.....	8
Some BYOD Examples and technical lessons learned by interviewed schools.....	9
Will your school's infrastructure support BYOD? Key questions to ask.....	13
Broadband provision .....	14
Sharing broadband connection amongst buildings or groups of schools.....	16
Wi-Fi network planning and deployment .....	16
Coverage .....	18
Capacity .....	18
Performance.....	19
Interference.....	19
Wireless transmission protocols.....	20
Internet Protocol version 6 (IPv6).....	20
Devices and applications.....	21
The performance advantages of filtering.....	23
Risk and security .....	23
Protecting the school network.....	23
Detecting unauthorised access points .....	24
User authentication.....	24
Device authentication .....	25
The security pros and cons of Virtual Private Networks .....	25
Safeguarding.....	26
Technical safeguarding tools and strategies .....	26
Student/staff circumvention of school network controls and safeguards .....	28
Banning mobile phones or banning the use of 3G/4G data connections? .....	29
Device and Application Management .....	30
MDMS and MAMS.....	30
Advising parents and students on purchasing BYOD devices .....	33
Preparation, maintenance and technical support for BYOD devices .....	34
Preparing devices for use in school .....	34
Maintenance of BYOD devices .....	35
Technical support for BYOD students.....	35



## BYOD Pocket Guide: Technical advice for school leaders and IT administrators

This is one of four shorter ‘pocket guides’ that has been developed from the full report, [\*Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators\*](#) that was published by European Schoolnet with support from Acer and the GSMA as part of the work of Ministries of Education in its Interactive Classroom Working Group (ICWG). It is designed for school leaders or new IT Administrators in schools that have decided to implement a Bring Your Own Device strategy and who are looking for practical, introductory advice regarding the technical aspects of doing this. The publication may also prove useful to more experienced IT Administrators who are interested in other schools’ experiences of BYOD implementations.

### Related pocket guides that you may find helpful:

- “BYOD Pocket Guide: An introduction to the technologies and terminology”
  - This pocket guide describes some of the technologies required to support BYOD, especially those associated with broadband and wireless networks. It is intended to provide a basic understanding of the technologies and jargon to enable school leaders to take part in informed discussions of key technical issues that will need to be addressed when planning and implementing BYOD.
- “Cloud computing and BYOD”
  - Using cloud based services in addition to BYOD increases the extent to which students can be both location and device independent.
- “BYOD Technical risks planning” - Planning for the introduction of BYOD should include a risk planning process. This guide describes some of the risks, their impact and how they might be prevented or mitigated.

## What do we mean by BYOD?

In schools and colleges BYOD usually means permitting students and teachers to bring personally owned devices (e.g. laptops, tablets, smartphones) into school to use these to access information, applications and services to support learning. To make technical and pedagogical support more manageable, schools may apply restrictions e.g. only allowing types and models of devices authorised for use in school. Alternatively, schools may advise a minimum specification for devices.

## Factors that affect BYOD technical requirements and options

As this diagram illustrates, technically and pedagogically there is no one-size-fits-all BYOD solution for schools.

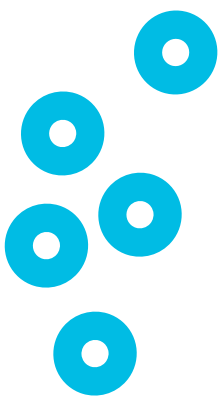
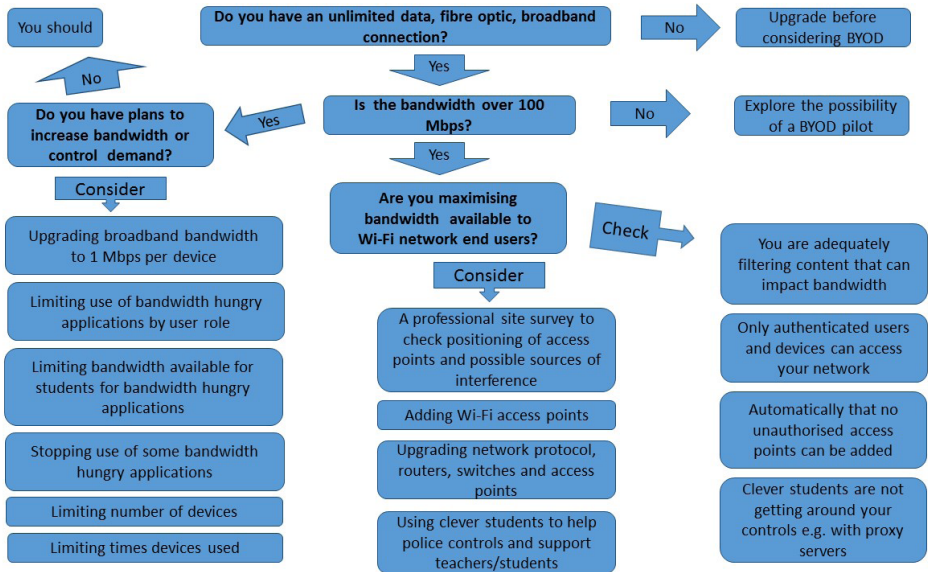


Many factors affect BYOD technical requirements and choices. The needs of a large, technical secondary school occupying several buildings in a European city are likely to be very different from the needs of a small rural primary school in another European country. Also, whilst some schools may appear superficially similar in terms of location, size and student age, their cultures and aspirations may differ considerably.



## Will our technical infrastructure support BYOD?

There will be many questions you will wish to ask concerning enhancements to your technical infrastructure required to support BYOD and strategies for coping with the infrastructure you have. Here are some key questions to get you started:



## Common technical challenges for schools implementing BYOD

Interviewees from several European countries were asked

*“In your experience, what are the three most common technical challenges facing schools in your country that want to implement a BYOD policy”.*

Their answers can be summarised as follows:

### Keeping up with developing requirements

- When planning to implement a BYOD policy it is important to consider the pedagogical objectives and the required functionality of the tools needed to support these before focusing on the detailed technical specifications of equipment.
- Having decided the pedagogical objectives and the BYOD model which will support these, the key objective of the technical planning is to assess the feasibility of the intended strategy. Some technical issues, if they cannot be solved, will mean implementation of BYOD should not go ahead e.g. if local internet service providers cannot provide a broadband connection with sufficient bandwidth.

### Connectivity and obtaining the necessary broadband speed

- The size of the challenge varies considerably dependent upon the location of the school.
- It is important to have more than just ‘entry level’ broadband.
- Schools implementing 100% BYOD need a very powerful Internet connection.
- A particular challenge can be achieving connectivity for the whole educational community - teachers, students, employees and parents - especially in difficult economic times.



## Wi-Fi coverage and capacity

- In planning for BYOD schools need to review their **Wi-Fi** coverage.
- Often existing WIFI coverage does not extend to all parts of the school building or buildings.
- If external funding or sponsorship can be found to upgrade Wi-Fi infrastructure this can help, especially for small schools which otherwise may not be able to meet the cost.
- **Access points** able to support high crowding (a high density of concurrent users in a location) may be required e.g. university campuses often use access points that support 128 devices.
- Many access points designed for offices cannot support the network traffic generated by classrooms full of students in a school.

## Device management

- Manual management of large numbers of student devices is time consuming and schools typically have limited IT administration resources.
- **Mobile Device Management Systems** can be very helpful but need client software to be installed on BYOD devices and require some technical expertise.

## Control of access via BYOD devices to educational and other content

- Various tools and strategies are needed to ensure only authorised devices can access school resources and that students can access the content they need for their studies easily and safely.

## Access to electricity supply

- Installing switches that support **PoE (Power over Ethernet)** technology and powering **Access Points** directly via **Cat 6 network cable** avoids the need and associated costs for a separate power socket to power each Access Point.
- Schools also need to make arrangements for charging devices during the school day if necessary

## Safeguarding students from potential on-line risks

- This is always a concern and a technical challenge for schools in all countries.
- **Internet filtering** is important as it reassures families, students and teachers.
- Technical safeguarding arrangements are of strategic importance as they can avoid something negative and easily avoidable becoming the sole topic of discussion and argument concerning BYOD and the use of the Internet in school.

## Acquiring devices to be used for BYOD

- Lack of financial resources for the whole educational community (including teachers, students, employees and parents) to acquire appropriate devices is a serious challenge in some countries.

## Switching to, or increasing the use of, web based learning materials

- This becomes a more urgent requirement when introducing BYOD and is important to ensure that students can work seamlessly on all their devices, at school and at home.
- The use of web based materials involves consideration of data protection which is an additional challenge added to that of access control to educational content.
- The increased use of cloud platforms by suppliers of text books and on-line learning materials can create work for teachers or IT Administrators. Teaching in a single subject may involve text books from up to five different publishers, and each publisher has their own cloud platform, schools have to register their students, create passwords, etc. for each one of these clouds.

## Mismatch between students and teachers expectations and knowledge

- In many schools issues arise due to the difference between highly motivated students, with mobile technologies they expect to use, and teaching staff who tend to be more conservative.
- Teachers need sufficient continuing professional development to help them adapt.





## Some BYOD Examples and technical lessons learned by interviewed schools

	Connectivity	Smart phone	Tablet	Notebook/Laptop	Min. Spec/Any	Model	Technical lessons learned
<b>SMALL SCHOOLS</b>							
Middle school, Austria	30 Mbps broadband. Small portable routers used to create ad-hoc Wi-Fi hot spots for a small number of devices.	Yes	Yes	No	Any	Classroom use only via temporary Wi-Fi hot spots	<p>Technical ingenuity and inexpensive tools enable BYOD experimentation when connectivity is very limited.</p> <p>“<i>Cloud computing is the future</i>”, the school plans to start using Google G Suite for Education soon.</p> <p>Regular training in computing, safety and security and independent working is needed for teachers and students.</p>
Primary/secondary school, Estonia	130 Mbps broadband. Separate Wi-Fi networks for BYOD and school-owned devices.	No	Yes	Yes	Any	Separate student BYOD Wi-Fi network with limited options and speed	<p>Install cabling all over the buildings to make it easy to add Wi-Fi access points when needed.</p> <p>Restrict access to social networking and file sharing sites on school network to save bandwidth.</p>

	Connectivity	Smart phone	Tablet	Notebook/Laptop	Min. Spec/Any	Model	Technical lessons learned
<b>SMALL SCHOOLS</b>							
Small secondary school, Switzerland	100 Mbps broadband	No	Yes, size 10+ inch	Yes	Min spec	BYOD voluntary, students can opt to attend “classic” classes with no technology use.	<p>Installing switches that support PoE (Power over Ethernet 31 W) means no need for additional electric sockets, therefore saves money and disruption.</p> <p>Training for teachers is important, limited technical knowledge of some has resulted in students being told to use learning materials not compatible with their iOS tablets.</p> <p>Cloud based services enable students to be both location and device independent.</p> <p>Printing will not disappear completely, “students like to have paper in their hands”, update printers to work over the network and enable printing from devices.</p> <p>“There are many tools to ‘protect’ students but it is always best to work out an eSafety strategy with them and educate them because they usually find work arounds when the barriers in place are only technical”.</p>

	Connectivity	Smart phone	Tablet	Notebook/Laptop	Min. Spec/Any	Model	Technical lessons learned
<b>LARGE SCHOOLS</b>							
Large technical secondary school, Italy	1Gbps broadband.	Yes, size 5 + inch	Yes	Yes	Any	School ensures all students have a device and a network that can support them. Then teachers decide whether or not to use devices in their lessons.	<p>It is best to experiment with BYOD over several years gradually increasing the number of students whilst incrementally upgrading the Wi-Fi network. Over time the school added access points and a management system with a controller to manage all the access points. Then the network was upgraded to <b>IEEE 802.11ac</b> protocol. Wi-Fi access 'liberalisation' followed with all students and staff able to access the network from any device.</p> <p>Installing a mirroring system on all Interactive Whiteboards allows any teacher or student device to project directly onto the board during lessons.</p> <p>Cloud based services and BYOD (with excellent broadband and Wi-Fi) delivers significant economic advantage to the school compared with school owned and managed servers and devices.</p>

	Connectivity	Smart phone	Tablet	Notebook/Laptop	Min. Spec/Any	Model	Technical lessons learned
<b>GROUPS OF SCHOOLS</b>							
Group of 14 schools, Portugal	1Gbps, minimum 100 Mbps per school	Yes	Yes	Yes	Any	BYOD devices used in most classes, if students do not have, or devices are not suitable, they use school tablets.	<p>Use centralised authentication (OpenLDAP) and access control (<b>Radius + 802.1X</b>) to control network access.</p> <p>Cap bandwidth available to groups of users according to their role and bandwidth available for specific applications within roles e.g. “give teachers lots for YouTube for teaching and students little for Facebook”.</p> <p>Use user profiles with filtering to prevent access to age inappropriate content.</p> <p>Using private clouds and open source tools to develop cloud based services; has cost and efficiency advantages but requires staff with technical knowledge and experience.</p> <p>Make parents/students responsible for their own tech support, IT literate teenagers can help each other and make videos for younger students.</p>

## Will your school's infrastructure support BYOD? Key questions to ask

A BYOD strategy will have the most obvious and immediate impact on a school's IT network services and the staff who support that network. Introducing BYOD, even when this is on a voluntary basis and/or involves only a few classes, increases the number of:

- users sharing internet bandwidth
- locations from which students and teachers use Wi-Fi to access the internet and school systems
- concurrent users accessing the Wi-Fi network
- potential concurrent users of mobile network cells
- items stored in and retrieved from cloud storage

Where schools have not anticipated these increases, problems with response times have quickly arisen, teachers and students have become frustrated and discouraged and BYOD has been seen as failed. The biggest challenge is designing, deploying and managing a new or enhanced Wi-Fi network which will consistently provide the level of service expected by students, teachers and other staff using BYOD devices, without degrading existing services. It will also be necessary to review broadband arrangements to ensure adequate bandwidth for an increased number of users and devices both immediately and in the longer term.

This diagram includes some key questions that need to be addressed when planning to implement BYOD. See the pocket guide "BYOD: An introduction to the technologies and terminology" if there are terms in the diagram that you do not understand.



## Broadband provision

Recommendations for school leaders from a previous ICWG project, published by EUN in “*BYOD – Bring your own device: A guide for school leaders*”, include “do not start without fast, robust connectivity”. The obvious questions this raises are “what is fast?” and “how do we ensure our service is fast and robust?”.

In some countries (e.g. Italy) school IT experts believe now is a good time to introduce BYOD because telecommunications operators are rapidly making available **FTTC and VDSL lines** that can guarantee download bandwidths of up to 1 **Gbps**. Both Italian and Portuguese experts interviewed recommended 1 Gbps bandwidth for large schools or groups of schools.

Some small schools have found that they are able to experiment with the use of a very basic BYOD model even with very modest bandwidth, as low as just 30 **Mbps**, by providing teachers with small portable Wi-Fi routers to create temporary Wi-Fi hotspots in classrooms for students’ devices to connect to.

**Generally the consensus view of European school-based experts interviewed can be summarised as:**



**The minimum bandwidth needed for a small school implementing BYOD is 100 Mbps increasing according to school size, number of devices and device use.**

**For a rough estimate of required bandwidth for a large school, or a group of schools, operating BYOD use 1Mbps per connected device (e.g. 1000 devices = 1 Gbps).**

Interviewees noted that currently in many cases schools do not have and will struggle to obtain the amount of bandwidth suggested by these rules of thumb. In view of this, they describe strategies for allocating bandwidth according to users’ roles and restricting the use of bandwidth hungry applications for some types of user.

NEN- The Education Network<sup>1</sup> in the UK suggested<sup>2</sup> a minimum bandwidth of 100 Mbps in 2013. However, even at that time they observed “The requirement for a 100 Mbps connection for a secondary school has already been exceeded in that the best connected schools in the



1 NEN –The Education Network provides support and advice to schools and local authorities and “works with industry and policy makers to provide advice, standards and support that will assist schools in making the right choices in the complicated and competitive arena of broadband provision”.

2 “Selecting Broadband Connectivity for Your School”, NEN-The Education Network, 2013



UK have 1 Gbps connections”. They also suggested a rule of thumb of 2 Mbps per connected device.

The updated SETDA report published in 2016<sup>3</sup> references a State of the States report<sup>4</sup> stating that “bandwidth demand is growing in K-12 public schools at a rate of over 50% per year and predicts that the typical school district will need to triple its bandwidth in the next three years”. Schools in the USA are organised into districts and SETDA recommend minimum bandwidths required to support “Student-Centered Learning” in small, medium and large school districts with targets for 2017/18 and 2020/21 school years (see table below) based on “research; analysis of data sets from districts across eight states regarding both capacity and usage; and consultation with experts in the field”.

Their recommendations for 2017/18 seem quite consistent with the rules of thumb suggested by interviewees for these guidelines.

School Year	2017-18 Targets	2020-21 Targets
<b>Small School District (fewer than 1,000 students)</b>	At least 1.5 Mbps per user (Minimum 100 Mbps for district)	At least 4.3 Mbps per user (Minimum 300 Mbps for district)
<b>Medium School District Size (3,000 students)</b>	At least 1.0 Gbps per 1,000 users <sup>^</sup>	At least 3.0 Gbps per 1,000 users
<b>Large School District (more than 10,000 students)</b>	At least 0.7 Gbps per 1,000 users	At least 2.0 Gbps per 1,000 users

*SETDA broadband capacity recommendations<sup>5</sup>*

Of course, in all schools the bandwidth available to individual teachers, students, other school staff and guests varies according to factors such as:

- The size and structure of school buildings.
- The total number of students, teachers and other staffs’ devices used in school, the number of devices being used simultaneously in specific areas of the school together with the number and capability of the access points being used to provide Wi-Fi connectivity to these.

3 Fox, C., Jones, R. (2016). The Broadband Imperative II: Equitable Access for Learning. Washington, DC: State Educational Technology Directors Association (SETDA)  
<http://www.setda.org/wp-content/uploads/2016/09/SETDA-Broadband-ImperativeII-Full-Documents-Sept-8-2016.pdf>

4 State of the States Report 2015.EducationSuperHighway. <http://stateofthestates.educationsuperhighway.org>

5 Fox, C., Jones, R. (2016). The Broadband Imperative II: Equitable Access for Learning. Washington, DC: State Educational Technology Directors Association (SETDA)

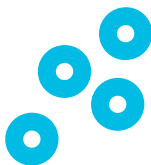
- The curriculum and the teaching methods employed and the resulting amount of on-line activity, especially the extent to which this includes downloading and uploading bandwidth hungry items such as high quality images and videos.
- The number and nature of administrative and site or facilities management systems using the network. In addition to Management Information, Learning Management and Registration Systems, this may increasingly include Internet-of-things-type applications involving remote monitoring and adjustment of heating, lighting, fire and flood alarms, security motion sensors, cameras and alarms.
- School policy regarding access to bandwidth hungry services e.g. do staff and students need to, and are they permitted to, access social networking sites like Facebook? How much are YouTube, video conferencing and cloud storage services used?
- The nature of administrative and operational processes, for example whether the school limits the amount of bandwidth available to some users of the network in order to give priority to others.

## Sharing broadband connection amongst buildings or groups of schools

If a school has more than one building, or is located within a group of schools, it may be necessary to share a broadband connection. Sharing of a broadband connection across multiple buildings can be achieved using one of the following:

- **Virtual Private Networks (VPNs)** and/or **Virtual Local Area Networks (VLANs)**
- Fibre optic cables
- Microwave connections, also known as radio bridges, where there is a line of sight.

In countries where **FTTC fibre optic** connections are now relatively inexpensive and widely available, sharing a connection among several buildings may not be necessary as it is just as cost effective for each building to have its own connection.



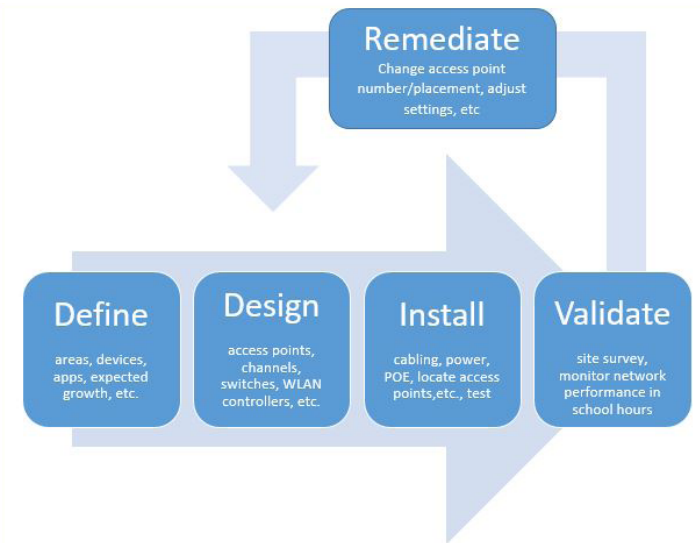


## Wi-Fi network planning and deployment

It is vital to carry out Wi-Fi planning at an early stage when planning to introduce or extend the use of BYOD in order to anticipate and later avoid or mitigate problems. It has been estimated that

“80% of new wireless networks will be obsolete within 18 months due to lack of proper planning<sup>6</sup>”.

Many organisations have documented processes for Wi-Fi planning and design, e.g:



*Wireless Network Design Process - based on Wireless LAN Professionals Inc. description<sup>7</sup>*

There are **automatic Wi-Fi network planner tools** available on the market and some networking companies and consultants recommend these at least to provide a first draft of the Wi-Fi network design. However, some school network managers have found these tools to be of limited use. Others suggest that it is never advisable to outsource planning of your wireless network and it is better to obtain advice and good practice examples from other schools that have practical experience.

6 Gartner Group quoted in “school wireless network design guide: what you need to know before you deploy a multimedia-grade school wireless network”, 2015

7 Diagram based on a process described in Parsons K R, “Why ‘One Access Point Per Classroom’ Approach is Wrong: A White Paper on Wireless LAN Design”, Wireless LAN Professionals, Inc., 2014

The Irish Government advise<sup>8</sup> that,

*“many Wi-Fi providers may not have sufficient experience of successfully implementing Wi-Fi in schools” and “The Wi-Fi requirements for post-primary schools are significantly different and more demanding than the requirements in business, home and other solutions”*

In Wi-Fi planning key considerations are coverage, capacity and performance.

## Coverage

Coverage refers to the areas where users and devices will be able to connect to the network. Consider whether these need to include outdoor as well as indoor areas, how many users are likely to wish to connect in each area and the minimum speed of service you will provide.

## Capacity

How many **wireless access points** will you need to be installed in each area? Each wireless access point can handle a certain maximum number of devices connecting to the network. Areas in which a large number of students can be connecting at the same time and making prolonged use of web or cloud based services, e.g. classrooms used for technology enhanced learning, will require more access points than areas in which there is only occasional use of Wi-Fi by a few people. How many access points are needed in a school is also dependent upon the type of access point used and how many users they can support. Advice from interviewees included:

- Cheaper devices, often purchased due to budget constraints or at a time when only limited use of Wi-Fi was anticipated, can only support 20 to 25 concurrent users.
- If cheaper access points are being used, a rule of thumb of one per classroom is unlikely to be sufficient to provide a good service for the teachers and students.
- More sophisticated and expensive access points can support up to 50 users.
- Dual band access points specifically designed for high user density areas are

8 “Guidance document for the provision of wireless network installations in post primary schools” Department of Education and Skills, Ireland (2016), <https://www.education.ie/en/School-Design/Technical-Guidance-Documents/Current-Technical-Guidance/Guidelines-for-Wireless-Networks-in-Post-Primary-Schools.pdf>



able to handle up to 128 users per band. These can provide a good service for three classes with some surplus capacity, which is useful when students arrive with more than one device e.g. a mobile phone and a laptop. They can also be used in busy areas e.g. canteens.

## Performance

Many factors, and some of the choices made when planning or extending a Wi-Fi network, can degrade or improve network performance. These include:

### Interference

Any intentional or unintentional **RF transmitters** - e.g. cordless phones, Bluetooth devices, existing Wi-Fi hot spots - using the same **frequency** as your Wi-Fi service can jam or degrade the service for students and other users. Identifying and eliminating sources of **RF interference** is one way to improve wireless network performance. When planning to introduce BYOD, commissioning a site survey to find out about the RF activity occurring already in and around the school helps with planning to provide good performance to the students and staff.

The Irish government<sup>9</sup>, advises that building structure

*“can be a significant area of challenge for schools. Most schools are constructed with concrete or brick walls, both of which attenuate (i.e. decrease the signal strength) of WLAN signals. Furthermore, when deploying WLAN into older or listed buildings, attenuation and cabling problems can dramatically increase and may require the deployment of more APs than initially planned”.*

Cisco advise

*“the recommended best practice for an optimal wireless deployment is to perform multiple site surveys to best understand and improve the RF environment”*

and suggest that organisations may benefit from commissioning “a professional

9 “Guidance document for the provision of wireless network installations in post primary schools” Department of Education and Skills, Ireland (2016), <https://www.education.ie/en/School-Design/Technical-Guidance-Documents/Current-Technical-Guidance/Guidelines-for-Wireless-Networks-in-Post-Primary-Schools.pdf>



site survey” involving a qualified wireless engineer. Some Access Points (e.g. Cisco Meraki Access Points) can be configured to broadcast a dedicated **SSID** for Site Surveys. Cisco provide guidance about carrying out a site survey using this SSID<sup>10</sup>.

Co-Channel Interference (CCI) or Co-Channel Contention (CCC)<sup>11</sup> where Access Points, and devices such as laptops, in close proximity can impact on each other’s communication, can also adversely affect Wi-Fi performance. Keith R. Parsons of Wireless Lan Professionals has warned<sup>12</sup> that one of the risks of the ‘one access point per classroom’ approach recommended by some suppliers is that, if no proper WLAN design process or post-installation validation survey is carried out, co-channel interference problems may be created.

## Wireless transmission protocols

The **wireless transmission protocol** used by school access points is important. IEEE 802.11N or IEEE 802.11AC protocol access points will support higher speed Wi-Fi, potentially **Gigabit** speeds. However, just replacing old access points with new ones that support IEEE 802.11N or IEEE 802.11AC will not, on its own, achieve the maximum performance improvement. When upgrading access points it is important ensure that switches used with these can also support gigabit speeds, otherwise the fastest speed will not be achievable. Nor will it be achievable by staff or students using computers or older mobile devices that are not compatible with these standards. Also, whilst IEEE 802.11N access points can operate in the **2.4 GHz** or the **5 GHz band**, IEEE 802.11AC access points only operate in the 5 GHz band which has a shorter range. Therefore, additional access points may be required and existing access point positioning will need revisiting.

## Internet Protocol version 6 (IPv6)

**IPv6** is the latest version of the protocol which specifies the format of packets of data and the addressing scheme for computers to communicate over the Internet. As well as providing more IP addresses than **IPv4**, IPv6 enables faster data transfer rates and can deliver significant security benefits.



- 10 [https://documentation.meraki.com/MR/WiFi\\_Basics\\_and\\_Best\\_Practices/Conducting\\_Site\\_Surveys\\_with\\_MR\\_Access\\_Points](https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Conducting_Site_Surveys_with_MR_Access_Points)
- 11 <http://www.tomcarpenter.net/2016/08/24/defining-wi-fi-cci-co-channel-interference-also-called-ccc-co-channel-contention/>
- 12 Parsons K R, “Why ‘One Access Point Per Classroom’ Approach is Wrong: A White Paper on Wireless LAN Design”, *Wireless LAN Professionals, Inc.*, 2014



Some schools are already working with IPv6, if they have a new network or if their network has been upgraded to IPv6. One interviewee recommends that IT Administrators prepare and save time when upgrading by allocating hardware addresses based on IPv6 even if the school's network is currently IPv4.

IT security company Sophos state that “All businesses should consider their IPv6 adoption plans, if they haven't already”<sup>13</sup>. They observe that services like Google and Facebook are currently available via IPv6, several large ISPs, telecommunications and web service providers are actively migrating and mobile operators have pushed for wider IPv6 implementation to support their high-speed networks.

However, they also advise “There are costs – both financial and in terms of manpower and effort – to making the switch to IPv6” which must be done correctly. Therefore schools should plan very carefully when and how upgrading will occur.

## Devices and applications

- What students and other staff are doing and what devices they are using, when they use the school Wi-Fi network, has a huge impact on network performance as some activities and applications use more bandwidth than others.
- It is important to know what devices and applications will be using a school's wireless network initially and in future to assess their impact on bandwidth.
- Wearable devices like smart watches, fitness trackers, smart glasses and virtual reality headsets are a fast growing personal technology trend. Some businesses are starting to have concerns about employees wearing these devices on commercial premises as they see them as a possible risk to the security of confidential data and few options are available for controlling employees' wearable BYOD devices (sometimes referred to as WYOD) as they have little, if any, user-manageable storage.
- Interviewees did not consider WYOD is likely to be a significant issue for schools in the near future and, as they communicate at very short-range with smartphones, they do not interfere with wireless networks.

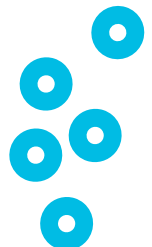
A number of strategies are employed by schools to control bandwidth utilisation by applications, e.g:

- Not allowing, or limiting within school, the use of the most resource hungry

13 <https://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx>

applications (e.g. those which involve streaming and uploading video and images) according to the profile of the user (teachers, students, administrators, parents, etc.) and possibly the time of day.

- If some applications are to be limited, or limited to certain times of the day only, consultation with teaching and other staff who may be affected is essential. Otherwise teachers who are innovative and trying to update their teaching can have their efforts derailed e.g:
  - Blocking YouTube in the mornings to reduce network traffic has disrupted lessons teachers had designed including learning activities using this application.
  - Blocking access to app stores prevents staff and students from downloading apps teachers wish their students to use.
  - Blocking websites related to computer games prevents teachers from researching the use of educational games.
- Capping the amount of bandwidth allocated to groups of users according to their role, and also capping the amount of bandwidth available for specific applications for users within these roles, can be helpful e.g giving teachers a lot of bandwidth for YouTube while allowing students just a little for Facebook.
- The bandwidth available for students using specific applications can be capped through the use of **traffic, or packet, shaping** tools.
- An essential planning tool is a simple table (see table) listing all known and anticipated devices (type and quantity) and the (on-line) applications expected to be used on these with each assigned a priority rating informed by:
  - The contribution an application being available on a specific device makes to the running of the school and/or to teaching and learning processes.
  - How demanding an application is on network resources e.g. voice and video require much more bandwidth than applications using only text and static images.



*Device and applications planning*

Device	Quantity	Application	Priority
Tablet PC – teachers	300	Class register system	1
		Moodle	1
		Student records system	1
		Internet (excluding YouTube and Facebook)	1
		Internet (YouTube)	1
		Internet (Facebook)	3
		Skype	2
Smartphone – teachers	200	Internet	1
		Moodle	1
Notebook PC - students	900	Moodle	1
		School Email	1
		Internet (excluding YouTube and Facebook)	1
		Internet (YouTube)	2
		Internet (Facebook)	4
etc., etc.			
<p><i>Priority 1 = essential to the running of the school; Priority 3 or 4 = would be nice if network can easily support</i></p>			

### The performance advantages of filtering

All schools will wish to apply content filtering to their internet service for child protection reasons. They will also wish to block adverts and malware which can be inappropriate, a danger to the network or wasteful of network resources. A useful side effect of filtering can be more efficient use of bandwidth as a great deal of rubbish is prevented from reaching the wireless network.



## Risk and security

### Protecting the school network

- Increased use of Wi-Fi in more areas in and around a school means increased risks to the network due to naïve, malicious or selfish actions by people within or external to the school. Actions to prevent or minimise these risks are related to ensuring only authorised access points and properly authenticated users and devices can access the network.
- Allowing only authenticated users to connect to the school's Wi-Fi avoids misuse and damage as well as the problem of people not connected with the school, e.g. people living nearby using the school Wi-Fi and thereby reducing the bandwidth available to students, teachers and staff.

### Detecting unauthorised access points

- If Wi-Fi network design includes connecting all Wi-Fi access points to a WLAN controller, as is common practice, the controller will constantly monitor them and detect any new access points that are not registered.
- Access points not registered with the controller may be “rogue” access points set up maliciously, by people wishing to hack the school’s network, or naively by teachers trying to save time by circumventing IT support without fully understanding the possible implications for the network.

### User authentication

- The simplest way of controlling access to wireless networks is the use of passwords. This is the typical approach in people’s homes or in public locations such as cafes. It is increasingly rare to have completely open access allowing anyone to connect to a network without any controls.
- Network security experts advise schools to use a single database of users and their credentials inside the network’s “directory services” to authenticate all users of school wired and wireless networks and to restrict their access to only the services they need to carry out their role in the school (i.e. Role Based Access Control or RBAC).
- A directory service is a component of a network operating system which maps the names of network users and resources to their network addresses.
- Individual user names and passwords is the usual approach in secondary schools. Interviewees have observed that, if every student has a personal



profile, it should be easy to identify any student who behaves inappropriately on-line

- There is some work involved in setting up profiles and allocating user names and passwords for all students at the beginning of each year.
- Some schools, especially primary schools, may not have individual user names and passwords for every student. This can be a deliberate policy to encourage use of on-line services with minimal barriers. Interviewees have commented this can be acceptable if wireless network coverage does not extend beyond the school.
- The Irish Government<sup>14</sup> advises schools to tell their Wi-Fi providers to adjust Wi-Fi coverage so that it does not extend beyond the external school boundary into public areas to reduce the risk of unauthorised Wi-Fi access.

## Device authentication

- One way of ensuring that only devices that are authorised can connect is the use of the Wi-Fi protocol **IEEE 802.1X** which ensures that devices seeking to access the network are authorised to do so by using an authentication (or RADIUS) server to consult a database to check this rather than simply requiring that the correct access key is provided.
- Schools can blacklist **IP addresses** that they do not want to access the school network, e.g. the addresses of **proxy servers** which students may use to bypass blocking of specific websites.
- Schools can **whitelist** IP addresses so that only devices with these addresses are able to gain access to the network.

## The security pros and cons of Virtual Private Networks

- A **Virtual Private Network (VPN)** can be used to ensure secure access to private school systems and data when students are using BYOD devices for learning outside school.
- Schools can also use private cloud based services to provide students, staff and parents with access to content and services from any location with Internet access.

14 "Guidance document for the provision of wireless network installations in post primary schools" Department of Education and Skills, Ireland (2016), <https://www.education.ie/en/School-Design/Technical-Guidance-Documents/Current-Technical-Guidance/Guidelines-for-Wireless-Networks-in-Post-Primary-Schools.pdf>



- Some interviewees have warned that **VPNs** need to be managed and many schools, especially at lower secondary or primary level, lack the expertise to do this.
- VPNs, like **proxy servers**, can also be a nuisance to school IT staff or service providers as they can be used by students to bypass school controls.
- Many VPN providers offer software that can be downloaded, often free of charge, to student devices and then used to access websites that students would not be allowed to access if the school network correctly identified them as students.
- Many students may have experience of using VPNs to circumvent controls some companies put in place to prevent their services being accessed outside specific geographic areas. Companies quite often try to prevent access from other countries e.g. the US version of Netflix is intended for use only within the USA but unofficial users in many countries use VPNs to make it appear that they are based in the USA in order to access it.
- If schools are aware that students are using, or might use, specific VPNs they can block these. However, as many VPNs are available, students may start using another. Alternatively, as VPNs use specific **network ports**, schools can use **port blocking** to prevent unauthorised VPN use.
- It is sometimes suggested that if organisations have upgraded to **IPv6** they will not need to use a VPN because IPv6 is rather like a VPN as it uses end-to-end encryption.
- Other experts suggest that there can still be advantages to using VPNs. However, many VPNs do not support or adequately support IPv6 and, if this is not understood and addressed, using IPv6 can be less rather than more secure than **IPv4**. Internet security company Sophos say, if done incorrectly, upgrading to IPv6 “can leave gaping security holes in your network systems” so “Don’t enable IPv6 until you’re fully ready<sup>15</sup>”.



15 <https://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx>



## Safeguarding

- The need to protect children in schools from inappropriate content and communication accessed via the Internet is a familiar topic for school leaders and IT staff.
- All schools will already have in place policies and strategies and advice for parents and students related to internet safety. The introduction of BYOD just increases the potential scale of existing issues as more student devices will be accessing the web from more locations within school.

## Technical safeguarding tools and strategies

There are different technical tools which IT Administrators or their service providers can employ to help to protect students from illegal, distasteful and age inappropriate content:

- **Firewalls, proxy servers** and **content filtering** are used to block unwanted content before it gets to the school Wi-Fi network users. In some countries ISPs supply schools with firewall and content filtering systems bundled with a fibre optic broadband connection for a single price. These tools are also included in managed services for schools.
- Filtering can include blacklisting specific apps and good filtering tools allow blocking of only certain services associated with a specific app.
- Some schools operate, or subscribe on-line to, **Mobile Device Management** or **Mobile Application Management systems** which include content filtering.
- Google search results are now **SSL encrypted**, as they say encrypting all transactions between search services and their users ensures these cannot easily be accessed by others. This change made it necessary for schools to revisit their content filtering arrangements to ensure students were still protected from inappropriate content, links to which could be in encrypted search results.
- Adding or activating **SSL interception**, also called **SSL Inspection**, functionality in school filtering solutions is a strategy suggested by NEN to address the issue of Google search results being protected by SSL). This means the filtering solution can intercept, decrypt, inspect and filter Google search results as well as Facebook and YouTube content which is also protected by SSL.

- In 2017 website hosting provider 1&1, used by many small businesses, is encouraging its customers to move to SSL. 1&1 is advising that that

“SSL encryption protects data transferred between your visitors and your website ...provides security and builds trust with your customer” and claim that “Google also ranks sites with SSL higher than those without”.

As more websites adopt SSL encryption, the use of SSL interception/Inspection by organisations, including schools, is likely to become more common.

- **Google SafeSearch**<sup>16</sup> is a useful safeguarding tool. However NEN –The Education Network warns

“It is important to recognise that SafeSearch does not offer the same level of granularity and control over filtering (for example, the ability to differentiate filtering by class, year group or role) that schools will currently enjoy via their discrete filtering solutions”.

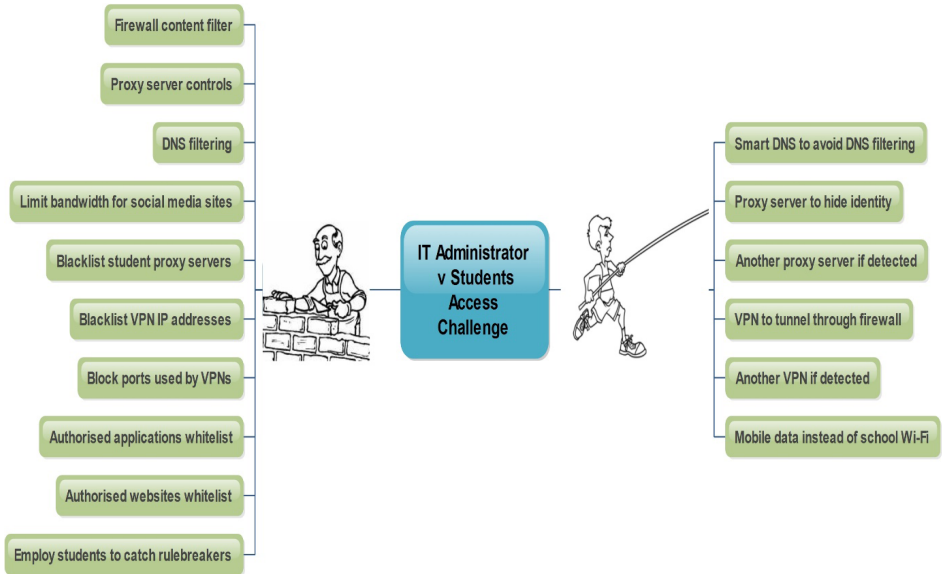
- **YouTube Kids**, available as IOS and Android apps, and the **Restricted Search** option on the YouTube website, attempt to filter out YouTube content that is unsuitable for children. However, these tools are not 100% successful.

## Student/staff circumvention of school network controls and safeguards

- Older, more technically literate students, and sometimes staff, often seek to circumvent restrictions put in place by IT Administrators and that this is more likely if more restrictive the controls are implemented.
- This can result in an “arms race” situation between IT administration and school network users with each advance made by the rule breakers needing to be countered by new security tools and strategies (see illustration).

<sup>16</sup> <https://en.wikipedia.org/wiki/SafeSearch>





- **Proxy servers** can be used by students to circumvent school controls, as well as by schools as part of their security arrangements. A 2009 BBC article about the use of proxy servers observed,

*“It sounds like an obscure, techy area of computing that only geeks would know about. But when we asked pupils in one secondary school classroom who had heard of proxy servers, every hand went up”<sup>17</sup>*

- Many websites openly advise students how to get around restrictions on what they can access on the Internet whilst at school.

*a Word to the Wise*

- **Advice from interviewees included working with students to develop an eSafety strategy and educating them about how important this is, especially as they usually find a way around technical barriers.**

17 <http://www.bbc.co.uk/newsbeat/article/10003579/pupils-bypassing-school-internet-security>

## Banning mobile phones or banning the use of 3G/4G data connections?

- In some schools, and in some countries, mobile phone use is banned in schools and BYOD devices do not include phones.
- Other schools have found that clear acceptable use rules, dialogue with parents and effective classroom management prevent significant problems from arising.
- Some schools only allow tablets that are Wi-Fi only and worry that if students have a mobile data contract they will use this to circumvent school controls and access unfiltered Internet (although European mobile network operators do block the most unsuitable Internet sites).



- **There is a growing consensus across European countries that a policy banning mobile phones is almost impossible to enforce now that most students in secondary schools, as well as many younger students, own a mobile phone.**
- It is sometimes suggested that schools could block mobile signals. Interviewees warn that, although this would be relatively easy, it is illegal in most European countries and there is a risk of interfering with school and nearby Wi-Fi services.
- Some IT Administrators observe that, if a large number of students simultaneously try to use their mobile data in school, they will probably block each other as mobile network cells can only support a limited number of concurrent users in a small area.



- **Encouraging students to use school Wi-Fi rather than mobile data is recommended by some IT Administrators. If students get good Wi-Fi for no charge they are likely to save their mobile data for no Wi-Fi areas.**
- Sometimes students being able to use their mobile data contracts can be an advantage to teachers and other students e.g. providing temporary Wi-Fi hotspots when a wireless network is down or if students are in temporary classrooms or outside school on field trips.

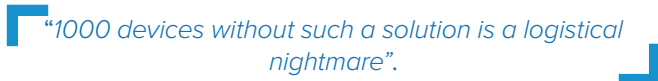
## Device and Application Management

- A key decision to be made is the level of responsibility, if any, the school will have for students' devices that may be damaged, lost or stolen.
- Associated decisions need to be made regarding who is responsible for, and how to arrange, device insurance, device tracking, locking - and perhaps remote wiping - of lost or stolen devices, replacement of lost, stolen or damaged devices and making available temporary loan devices.
- There are varying levels of cost and administrative or technical effort associated with these arrangements. If a school's BYOD model includes providing technical support for the students' mobile devices, the school may decide to implement a **Mobile Device Management System**.

### MDMS and MAMS

- A Mobile Device Management System (MDMS) is software that helps network managers to integrate mobile devices, such as smartphones, tablets and laptops, into a company's or school's network and to monitor, control and manage these. In order to do this, client software needs to be installed on each mobile device.
- MDMS allows distribution of applications, data, configuration settings and patches to all devices very quickly and easily from a central network location. Use of wireless networks for this distribution is sometimes referred to as OTA or Over The Air distribution.
- OTA enables schools to distribute textbooks and software licence keys in one click and deactivate these keys at the end of the school year.
- MDMS can save IT staff a great deal of time carrying out routine device administration and maintenance.
- MDMS enable monitoring of how and where the devices are being used. If one is stolen it can be locked and/or blocked from accessing the network and the data on it can be remotely wiped. Devices can also be remotely backed up and restored.
- MDMS is useful for schools, especially larger schools, that have given laptops, netbooks or tablets to their students or operate the type of BYOD model where parents purchase a specific device from, or recommended by, the school which

is then supported by school IT staff. One interviewee commented that managing

“1000 devices without such a solution is a logistical nightmare”.

- In some countries the use of MDMS in schools is controversial. Particularly where the BYOD model is that students bring in and use in school their personal mobile devices. Concerns have been raised about systems which enable schools to monitor what students’ do on-line outside school and to effectively monitor where they go.
- There can also be problems with monitoring students’ use of devices within school. An article providing legal advice to school administrators in the USA advises that there have been court cases as a result of schools monitoring students’ devices and then taking disciplinary action.<sup>18</sup>
- Schools that use MDMS with student owned devices need to ensure that students’ personal data is protected e.g. will not be deleted by remote software updates.
- Some suppliers advise schools that MDMS is “very important” or “vital” for child safeguarding. However, whilst access to inappropriate content is an area of concern for all schools, there are many strategies and tools used by schools to address this which may, or may not, include the use of MDMS.
- One interviewee warns that weakness of using MDMS with BYOD is a technically aware students may decide to uninstall the MDMS client from their device.
- **Mobile Application Management systems** (MAMS) may be the answer to the most common objection to MDMS, i.e. that they give IT staff too much control over BYOD devices, whilst delivering some of the advantages of MDMS around protecting data and systems.
- MAMS allow IT Administrators to deliver applications to multiple mobile devices and to control application configuration, updating and usage tracking.
- MAMS also monitor application performance and can delete mobile apps and data from an end user’s device remotely if the device is lost or when a student leaves.

18 Bathon, J, “Your iPad Rollout Could Get You Sued”, The Journal.com, 2013, <https://thejournal.com/articles/2013/09/02/your-ipad-rollout-could-get-you-sued.aspx?=THEMOB>





- MAMS does not require installation of client software on students' mobile devices, nor does it interfere with personal applications and data on the devices.
- Combined MDMS and MAMS products are available and used by some large schools.
- Where the BYOD model is students bringing in any device, schools typically expect students to manage their devices by themselves and to be responsible for downloading and updating necessary tools.
- MDMS and MAMS systems are rather complex to implement and manage and many, especially smaller, schools are unlikely to have sufficient IT expertise to do so. An easier and cheaper alternative can be to subscribe to a cloud based **SaaS** MDMS/MAMS.
- A regional ICT centre in Switzerland compared the cost for a school of 1000 students, 100 teachers and 2 school buildings of purchasing and maintaining an MDMS/MAMS (40,000 Swiss Francs to set up plus annual costs of 10,000 Swiss Francs) with the cost of subscribing to a cloud based service (16,500 Swiss Francs per annum).
- Some companies are implementing **containerisation**, which enables separation of corporate apps and data from employee apps and data on employees' BYOD devices with the IT department only controlling the contents of the corporate "container". Containerisation is relatively expensive and generally schools are not considering this approach. It has been mentioned as possibly something to consider in future but the increasing availability of SaaS MDMS/MAM solutions may make this unnecessary.

## Advising parents and students on purchasing BYOD devices

The amount of advice and assistance schools, or local/regional education authorities, give to parents and students regarding the purchase of mobile devices ranges from no advice at all to funding projects that research and test, and may even commission or procure, devices on behalf of parents.

As long ago as 2003 the Learning2go project in the UK, involved working with device manufacturers on the specification for netbooks to be purchased by parents to support teaching and learning in school. National, regional or local authorities in many countries have recommended, or purchased for students, specific consumer ICT devices e.g. Asus netbooks, Apple iPads, etc.

One of the biggest BYOD deployments in Europe, involving more than 300 schools and 24,000 students in the Catalonia region of Spain, started as a public education project (EDUCAT) to promote digital learning in 2009. When funding stopped in 2011 due to the economic crisis, the initiative continued with the support of parents and schools. The EDUCAT BYOD model involves all students using the same type of device, currently netbooks, that are paid for by parents. The schools involved test and compare devices and make recommendations; the decision of which devices to purchase is then made by parents usually via the Parents Association in each school. When testing devices the schools:

- Benchmark performance.
- Test battery life (the requirement is not less than 8 hours between charges).
- Assess reliability and robustness

The device currently in use in EDUCAT schools, the Acer TravelMate B1, was selected partially due to its ruggedized frame including a rubber strip to protect from bumps and drops, a strong hinge, cover that can withstand up to 60 kg of pressure, spill-resistant keyboard, non-glare screen and relatively light weight.

By working with the supplier, EDUCAT schools have obtained a device which is more robust than consumer products designed for home usage and can withstand the rigours of everyday use in schools. The schools have also negotiated with the supplier an extended warranty and a service support, including a dedicated service phone line which can be used by parents, schools or solution integrators to access help quickly if problems arise.

When selecting BYOD devices, Wi-Fi performance is a key consideration. The devices selected by EDUCAT schools use the **802.11ac** wireless protocol with **2x2 MIMO**, to achieve faster network connections (the supplier claims three times faster) than achieved by devices using the **802.11n** protocol.

## Preparation, maintenance and technical support for BYOD devices

### Preparing devices for use in school

Many schools issue guidelines to parents and students detailing, not only the minimum specification for BYOD devices, but also the preparation that must be



carried out prior to these devices being brought into school.

If BYOD devices are laptops, this guidance may include instructions to install:

- A specific version of an operating system (e.g. Windows 10)
- A specific Internet browser (e.g. Chrome)
- A specific version of office software (e.g. Office 2016)
- Anti-virus software
- Anti-malware software

In the case of tablets and smartphones, students may be instructed to:

- Ensure the device operating system has been updated to the latest version (e.g. iOS updates).
- install specific apps or ensure the latest updates for these have been applied.

Some of these rules are needed to avoid wasting school bandwidth on maintenance tasks which can be carried out at home by students.

## Maintenance of BYOD devices

There are a number of possible alternative approaches to maintenance of students' devices, e.g:

- Making maintenance the responsibility of the student.
- The school, or local education authority, negotiate on behalf of students/parents for a support service to be included in the cost of the devices purchased or covered by an insurance policy.
- The school dictates the specific device to be purchased by parents and the school is responsible for device maintenance.



Interviewees’ advice includes:



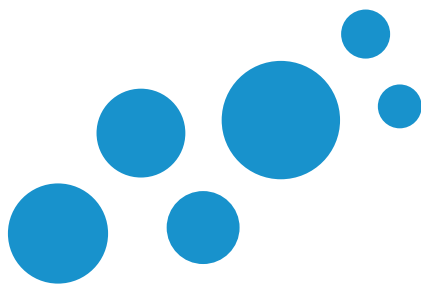
- **Make students responsible for downloading necessary tools and distribute most content via web interfaces.**
- **Avoid wasting school bandwidth, and time, on set up and maintenance tasks which can be carried out at home by students.**
- **Compile and share with teachers and parents lists of the apps and books that will be used in school and request that these are installed or downloaded at home ready for use in school.**
- **Have an agreement that students bring to school a device with the required software/apps installed, the latest updates applied, no viruses or malware and the batteries fully charged.**

### Technical support for BYOD students

- Early BYOD implementations in schools often included arrangements for schools to provide technical support for student’s devices and 1:1 computing implementations often still do, especially where this is managed by an external supplier.
- Schools are increasingly seeing device related technical support as something that students and their families should take responsibility for. This is partly due to the increased ubiquity and reliability of the consumer IT devices students now mostly use and partly due to the number of student devices involved; in some cases students may be bringing three devices into school - a tablet, a smartphone and a laptop.
- Technical support related directly to the functioning and use of a school’s IT network is still seen as the school’s, or their service provider’s, responsibility.



- **Interviewees suggested using and rewarding technically adept students to assist their peers, teachers and the IT administrator.**





Future  
Classroom Lab  
by European Schoolnet

# Bring Your Own Device for Schools

## Pocket Guide: Technical advice for school leaders and IT administrators

This is one of four shorter 'pocket guides' that has been developed from the full report, Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators that was published by European Schoolnet with support from Acer and the GSMA as part of the work of Ministries of Education in its Interactive Classroom Working Group (ICWG). It is designed for school leaders or new IT Administrators in schools that have decided to implement a Bring Your Own Device strategy and who are looking for practical, introductory advice regarding the technical aspects of doing this. The publication may also prove useful to more experienced IT Administrators who are interested in other schools' experiences of BYOD implementations.



<http://fcl.eun.org/icwg>