Bring Your Own Device
FOR SCHOOLS

Future Classroom Lab by European Schoolnet

Technical advice for school leaders and IT administrators
## Is this the right publication for you?

<table>
<thead>
<tr>
<th>IF YOU ARE</th>
<th>READ THIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>A school leader, or an IT Administrator, in a school that has decided to implement BYOD and you are looking for practical introductory advice regarding the technical aspects of this. Or you may be an experienced IT Administrator who is interested in other schools' experiences of implementation.</td>
<td>This is the publication for you</td>
</tr>
</tbody>
</table>

### DESIGNING THE FUTURE CLASSROOM

A school Head, IT Administrator, Teacher (or perhaps policy maker) who is not yet committed to implementing BYOD but wishes to learn more about the benefits and challenges of BYOD for schools and how these have been addressed by other schools around Europe, including consideration of pedagogy, inclusion and safeguarding.

---

**AUTHOR**
Jill Attewell

**EDITOR**
Jim Ayre

**PUBLISHER**
European Schoolnet (EUN Partnership AISBL)
Rue de Trèves 61
1040 Brussels
Belgium
www.eun.org

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License: http://creativecommons.org/licenses/by-sa/3.0/

**ABOUT THE PUBLICATION**
The report is created by European Schoolnet's Interactive Classroom Working Group (ICWG) with support from Acer and the GSMA. The ICWG's aim is to explore common areas of concern, share experience, and address policy challenges related to the integration of a wide range of technologies in classrooms and their impact on teaching and learning. Ten Ministries of Education are involved (Austria, Czech Republic, Estonia, Ireland, Italy, Luxembourg, Norway, Portugal, Switzerland, Turkey). Read more at fcl.eun.org/icwg

**PICTURE CREDITS**
From Shutterstock.com: Syda Productions (p. 41);
From Acer: pp. cover-7-17-20-49

**ORIGINAL DESIGN**
Karakas Graphic Communications, Brussels

**DTP**
Jessica Massini

**PUBLISHED**
August 2017

All links have been checked at the time of publication. The reference to the website does not constitute an endorsement of the product or organisation.
BYOD for Schools: Technical advice for school leaders and IT administrators
In education BYOD or Bring Your Own Device is commonly used to mean permitting students and teachers to bring personally owned mobile devices (laptops, netbooks, tablets, smartphones, etc.) into educational institutions and to use those devices to access institutional information, applications and services in order to support learning.

To make technical and pedagogical support more manageable, schools often apply restrictions; for example, only allowing students to bring in the types and models of mobile device that have been authorised for use in school. Alternatively, schools may advise a minimum specification for devices.

In some schools BYOD may begin in an informal, ad-hoc way as a few teachers begin to recognise that students’ own devices could be useful in the classroom. Alternatively, introduction may be the carefully planned, strictly controlled and monitored process of implementing a whole school strategy with clear aims and objectives. There is no one-size-fits-all BYOD solution for schools. The needs of a large, technical secondary school occupying several buildings in a city are likely to be very different from the needs of a small rural primary school in another country even within Europe.

The technical challenges of facilitating and managing BYOD also vary greatly dependent upon many factors including:

- the culture, norms and laws related to the use of mobile devices in schools in a country
- a school’s size, age, location, construction, infrastructure, previous and current use of technology and the subject areas it specialises in
- the availability of technically expert staff

The decision to introduce BYOD will have the most obvious and most immediate impact on a school’s IT network services and the staff who support that network. The introduction of BYOD, even on a voluntary basis or involving only a few classes, increases the number of:

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

Where schools have not anticipated these increases, problems with network access and response times have quickly arisen, teachers and students have become frustrated and discouraged and BYOD has been seen as having failed.

The biggest technical challenge is designing, deploying and managing a new or enhanced Wi-Fi network which will consistently, safely and securely provide the level of service expected by students, teachers and other staff using BYOD devices, without degrading existing services. It is also necessary to review broadband arrangements to ensure adequate bandwidth for an increased number of users and devices both immediately and in the longer term.

A section early in this document contains explanations of some basic concepts and common terms or acronyms to assist understanding of the later discussions of infrastructure requirements, Wi-Fi planning and device management.

There are many questions that school leaders should ask and/or encourage IT staff to investigate when planning to implement BYOD. The following diagram includes some key questions that need to be addressed and further discussion of these can be found in the sections of this document cross referenced.
Do not worry if you do not understand some of the terms used in the diagram now. As you read on, these will be introduced and explained.
1. Introduction

1.1. Background

This guide has been developed by European Schoolnet (EUN) as part of the work of Ministries of Education in its Interactive Classroom Working Group (ICWG) following on from the research which informed production of the 2015 EUN publication “BYOD, Bring Your Own Device, A guide for school leaders”.

A number of interviewees who participated in the original project, at both school and local/region level, expressed the opinion that advice on the technical aspects of introducing and managing BYOD would be helpful. However, beyond providing some very generic advice and a few pointers, neither the timescales nor the objectives of that initial project were sufficient to enable this request to be addressed.

1.2. Methodology

The methodology used to collect data for this resource included:

- A literature review drawing on the findings of research funded by governments and groups of governments, published academic papers, commercial white papers and more informal online sources.
- Interviews with school based IT or network managers, educational technologists and experts in national and regional education authorities (see Section 12 Acknowledgements).

1.3. Aims and target audience

The aims of this publication are:

for School Leaders:

- to provide school leaders who have limited relevant technical knowledge with information which will allow them to engage in informed requirements analysis, planning and on-going oversight of the technical aspects and implications of BYOD; and
- to provide school leaders who have some relevant technical knowledge with useful reminders and tips plus links to additional, regularly updated information and best practice examples.

for School IT Administrators:

- to provide new school IT Administrators who do not have substantial previous IT experience or formal IT qualifications with some relevant technical information and advice plus links to additional, regularly updated information and best practice examples.
- highly qualified school IT Administrators may find some of the examples and tips useful and may appreciate links to additional, regularly updated information and best practice examples.

The outcomes and outputs of the project may also be useful to support agencies and policy makers at local, regional and national levels.

1 Blamire R and Colin J N. “The School IT Administrator: analysing the profile, role and training needs of network administrators in Europe’s schools”, EUN 2015.
1.4. What do we mean by BYOD?

In education BYOD/Bring Your Own Device (or BYOT/Bring Your Own Technology) is commonly used to mean permitting students and/or staff to bring personally owned mobile devices (laptops, netbooks, tablets, smartphones, etc.) into educational institutions and to use those devices to access institutional information, applications and services.

Educational institutions often provide ‘guest’ access to a Wi-Fi network for visitors or contractors. This may be a separate network and usually provides access to no more than the public Internet. This type of access may sometimes be included in definitions of BYOD but is a very limited type of BYOD. It may also exist in addition to more comprehensive models. School BYOD strategies may, and it can be argued should, go further than merely allowing students to use their own mobile devices in school and providing some internet access for them. A more beneficial approach involves embedding the use of students’ own devices into teaching and learning both within and outside the school.

School BYOD strategies may require parents or guardians to purchase mobile devices for students to bring into school. This approach can help to make technology enhanced learning more affordable for schools and more sustainable in the long term. Supporters argue that parents often provide other equipment and stationery for use in school, so why not mobile devices? However, this can be controversial, especially if parents are inadequately consulted or have concerns about the cost. Also, in some countries, parents contributing to the cost of education is thought to undermine the principle of free education and in this context there may be resistance to BYOD. A common approach is for schools to implement schemes which assist parents, or the students themselves, to purchase mobile devices at discounted prices and, in some cases, to pay for these in instalments.

Research for these guidelines, seems to suggest (although more data and analysis would be required to confirm this) some relaxing of attitudes of school leaders and IT staff may be occurring towards students using in school whatever mobile device they happen to personally own. This may be due to the use of smartphones and tablets becoming so much a part of everyday normal life for teachers, parents and students in European countries that excluding them from school seems not only strange but wasteful.

To make technical and pedagogical support more manageable, schools often apply restrictions; for example, only allowing students to bring in the types and models of mobile device that have been authorised for use in school. Alternatively, schools may advise a minimum specification for devices to make them acceptable for use in school. When schools dictate technical specifications for devices to ensure all students have the same, or similar, devices this makes life easier for teachers and technical support staff and helps them to feel more comfortable with, and therefore more accepting of, the culture change involved.

Possibly the most easily managed but more restrictive approach, not always included in definitions of BYOD, is when a school arranges for parents to buy into a 1:1 mobile computing managed service provided by an external supplier. One example is the service provided by Wriggle to many schools in Ireland, where state schools generally do not have in-house IT Administrators and would therefore find it difficult to manage other BYOD models.

Finding the right balance between control and risk/support complexity (see figure 1) and deciding what are acceptable levels of risk are key elements in the development of a school BYOD strategy.

http://www.wriggle.ie/
A new acronym starting to appear in the corporate world is WYOD (Wear Your Own Device) and some IT staff in educational institutions are starting to consider the implications of students’ use of wearable devices, including smart wristbands and augmented/virtual reality glasses/headsets, including any impact on school networks. In Switzerland there has been some concern expressed about the potential for “cheating with wearable devices in upper secondary schools” and some interviewees noted that they could add to the total number of devices sharing the school’s broadband but, Dario Zucchini, the Digital Coordinator at the Industrial Technical Institute Majorana of Grugliasco (ITIMG) in Turin in Italy advises, “these are tools that communicate short-range, with your smartphone. Therefore, they don’t interfere with the Wi-Fi network.”

1.5. Some BYOD Scenarios

In some schools BYOD may begin in an informal, ad-hoc way as a few teachers begin to recognise that students’ own devices could be useful in the classroom. Alternatively, introduction may be the carefully planned, strictly controlled and monitored process of implementing a whole school strategy with clear aims and objectives. The following are some examples of possible BYOD scenarios:

**Informal single teacher scenario**
- One school teacher allows students to bring their smartphones into classes and collaborates with them to find ways to use these to support learning.
- The teacher is motivated by a desire to try something different or to engage hard to reach students.
- The teacher does not seek permission and may even be acting against official school policy; school leaders may be unaware BYOD is occurring.
- The teacher may or may not share information with other teachers and encourage others to try BYOD but, if they do, BYOD can slowly spread and some benefit will be seen.
- Impact on teaching and learning is dependent upon an individual teacher’s ability to enthuse others and all BYOD may cease if that teacher leaves.
- Also, if the teacher finds a way of unofficially providing Wi-Fi access for the students’ devices, they may not realise that this could have a negative impact on the service available to other network users.
Some schools have a mixed approach. At Gymnase Intercantonal de la Broye school in Switzerland, for example, the school advises a minimum specification for devices parents should purchase to support their child's learning and also allows students to bring in any device they own. Philippe Devaud, who is an IT Adviser in the Department of Education’s regional ICT Centre, says the reason for this policy is,

“because a lot of students already own devices by the time they start grammar school [and] parents prefer this approach [so it is the] path of least resistance”.

However, these additional student owned devices are only able to access limited services within the school.

Voluntary BYOD for older students scenario

- A school principal decides to allow students in the senior years to bring mobile devices into school to support their learning.
- Teachers are encouraged but not required to allow use of the mobile devices in their classes.
- Teachers are offered technical training and may attend workshops on the pedagogical uses of mobile devices if they are interested.
- IT department/administrator does not have any responsibility for the students’ mobile devices but does allow connection to a school Wi-Fi network.
- Some ICT literate students are rewarded for providing support for their peers and advice to teachers.
- Pockets of good practice will develop and some students will benefit, some students will not bring devices to school and some teachers will not allow use in their classrooms or will not fully exploit the potential of the students’ devices to enhance teaching and learning.
- If many teachers and students do take up BYOD the additional demand on the Wi-Fi network and school broadband bandwidth will present challenges for IT staff and may cause frustration and disillusion amongst students and teachers who will not be able to operate as they had hoped.

Planned and controlled whole school tablet scenario

- A secondary school principal decides in consultation with teachers, IT staff and other stakeholders to require all parents to fund tablets for their children to make the introduction of tablets for teaching and learning affordable and sustainable.
- In order to make technical support by school IT staff and staff training as easy as possible, to avoid any parental or societal concerns about potential inequalities and to obtain an attractive price for parents due to bulk purchasing, it is decided that just a few devices types/models will be used.
- A project team plans and oversees implementation of a school wide BYOD strategy.
- The school invests in enhanced broadband and upgrades the Wi-Fi network to cater for the planned increase in traffic.
- Arrangements for IT support are reviewed and enhanced as required. This may include recruiting additional staff, providing extra staff training and/or outsourcing some support services.
- Training courses and workshops plus both technological and pedagogical support are arranged for teachers. All teachers are informed that they will be required to use the tablets in their lessons. Arrangements are made to monitor progress and evaluate impact.
- BYOD is likely to be successfully implemented throughout the school. Although there may be issues with IT staff and some teachers wishing to restrict how and when devices and online services are used whilst students and other teachers may want more freedom to use devices and services as and when they wish. Also students may feel less ownership as the type of device was dictated by the school.

Some schools have a mixed approach. At Gymnase Intercantonal de la Broye school in Switzerland, for example, the school advises a minimum specification for devices parents should purchase to support their child's learning and also allows students to bring in any device they own. Philippe Devaud, who is an IT Adviser in the Department of Education’s regional ICT Centre, says the reason for this policy is,
1.6. How IT services are supported in schools and the challenge of BYOD

1.6.1. The IT Administrator

The introduction to the European Schoolnet/Cisco publication about School IT Administrators\(^3\) observes

"Across Europe, and for many years now, governments, regions and schools have been making significant investments in ICT connectivity, equipment and services in order to make digital age teaching and learning a reality for young people, and to equip them with the competences needed to thrive in the 21st century. The people in schools who are responsible for maintaining and upgrading the technological infrastructure occupy an increasingly vital role in ensuring that this investment pays dividends".

The authors of this study define the school IT Administrator as follows:

"...in some countries known as the network manager, systems coordinator or IT manager – is the person in the school who oversees the technical development and implementation of IT, for example administering the network, managing devices in the school, addressing security issues and providing technical support to teachers. It is distinct from the ICT coordinator, or e-learning manager, who has a more pedagogical role".

In some schools in some countries there may not be school based IT managers or IT support may be a part time responsibility of one of the teachers. Alternatively there may be IT staff who are very limited in the support they can, or are allowed to, provide with more complex matters being the responsibility of local or regional support teams. There are also many schools that outsource some or all of their IT services to an external supplier.

Therefore, the level and location at which decisions about BYOD and the technical aspects of how it is managed and supported can vary a great deal.

When school IT advisors were surveyed by Blamire and Colin the most mentioned challenges they faced were "security, BYOD management, IT management, staff support and development".

The culture change of BYOD can be difficult for school based IT staff and this may make them unenthusiastic about plans to introduce BYOD. There are several reasons for this:

- Worries that increased demand on the network and bandwidth and the potential negative impact on school systems.
- A reluctance to give up some of their traditional control of all aspects of IT within the school.
- Concern that, if problems arise, they will be blamed.
- Concern about additional workload e.g. the need to register all student devices at the beginning of each academic year.
- Worries that if students are responsible for their own device maintenance and support, IT staff jobs could be threatened.

Schools which have successfully introduced BYOD or other mobile learning initiatives recommend involving IT support staff (or external providers of IT support) early in the planning stages, asking for their advice, providing them with devices to research potential issues and solutions and encouraging them to communicate with and learn from other schools’ experiences.

If a school’s BYOD strategy includes responsibility for supporting the students’ devices, the number and knowledge of IT staff currently employed may be insufficient, necessitating additional investment in staff and staff training or outsourcing of IT support to a company or organisation that provides a “managed service”.

\(^3\) Blamire R and Colin J N. "The School IT Administrator: Analysing the profile, role and training needs of network administrators in Europe’s schools", EUN 2015
1.6.2. Local Area or Regional IT Support

In many countries there is a shortage of school based IT support, particularly network management, expertise. Traditionally the extent to which information technology has been used in schools has typically been insufficient to justify the cost of employing an IT manager for every school. Therefore, IT support is often organised at local or regional level with policy related infrastructure, Internet access and sometimes the type of devices to be used, being made at national level.

There are clear advantages to this approach in that dedicated teams of experts are able to research the most appropriate technology for their schools, develop policy, plan roll out of equipment and provide on-going support, advice and monitoring with costs being met from central budgets rather than by individual schools.

However, centralised technology policy and services departments can be rather conservative and can be slow to react to changing technological and social contexts.

National and regional policies can be informed and kept up-to-date by learning from the experiences of schools which have implemented BYOD successfully and lessons learned and good practice can be shared with other schools.

1.6.3. Outsourcing BYOD

In some cases the whole BYOD, or 1:1 computing, service is outsourced to a managed service provider.

The Irish schools who are supported by the managed service provider Wriggle seek advice from the company and discuss their vision and requirements. They decide upon the type of device they will require every student to bring in (e.g. an iPad tablet, Microsoft Surface, etc.) and parents then purchase a service directly from Wriggle, via a web portal, including a device, the learning materials and apps agreed with the school, a managed service including a cloud based Mobile Device Management System and technical support. The company delivers teacher development workshops in schools to help them prepare for the introduction of the devices and their use for supporting teaching and learning.

Wriggle do not supply, upgrade or support schools’ broadband and Wi-Fi infrastructure. However, they do tell schools they need an enterprise standard Wi-Fi network managed by WLAN controllers (see Section 6.1.2.5) and advise a rule of thumb of one Access Point (see Section 6.1.2.5) per classroom. Wriggle also review the existing infrastructure with the school and may help to review quotes from network suppliers. Wriggle advise whether the current or proposed Wi-Fi network is sufficient to support their managed service.
2. Factors that affect BYOD technical requirements and options

From the technical, as well as the pedagogical, point of view there is no one-size-fits-all BYOD solution for schools. The needs of a large, technical secondary school occupying several buildings in one European city are likely to be very different from the needs of a small rural primary school in another country even within Europe. Furthermore, when schools appear superficially similar in terms of location, size and student age their institutional culture and aspirations may differ considerably. There are many factors which affect the BYOD technical requirements, choices and decisions for a school (see figure 2).

Figure 2: Factors affecting BYOD Technical Choices
3. The most 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** was one of the challenges suggested by our Austrian interviewee. 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 (e.g. the learning management system) “AND then you can think about technical equipment” needed to achieve the pedagogical objectives. Georg Koeck, IT administrator and eLearning lecturer at New Middle School Lienz-Nord emphasized. Many sources and interviewees make it clear that, having decided upon the pedagogical objectives and the BYOD model which will support these, the first key objective of the technical planning is to assess the feasibility of the intended strategy. This is because some technical issues, if they cannot be solved, will mean implementation of BYOD should not go ahead. Perhaps the most obvious of these would be if local internet service providers cannot provide a broadband connection with sufficient bandwidth.

- **Connectivity and obtaining the necessary broadband speed** were mentioned as key challenges by interviewees in Estonia, Italy, Portugal and Switzerland and the size of the challenge varies considerably dependent upon which part of which country a school is located in. Dario Zucchini of ITIMG school in Italy commented that his suggestions might not be the most common challenges but they are the most significant “in the sense that if you mess them up BYOD doesn’t work” and the first of these was connectivity. It is important to have more than just ‘entry level’ broadband. This is a good time to be upgrading your connectivity [in Italy] because fibre optic FTTC connections are increasingly available in many areas. Dario reports that in Italy...

“for around 50 Euros per month you can purchase 100Mbps of bandwidth ... for the price of a sack of potatoes you can get connectivity that only large companies had before”.

António Paulo Santos, Director of computer facilities at the Carlos Amarante group of schools in Portugal added that a particular challenge is achieving...

“Connectivity for the whole educational community - teachers, students, employees and parents”,

especially in difficult economic times. In some communities in Portugal...

“many parents don’t have connectivity or smartphones or tablets”.

Philippe Devaud, IT Adviser in the Department of Education’s regional ICT Centre, noted that the challenge in Switzerland is, “A school that wants to go 100% BYOD needs a very powerful Internet connection. These are expensive and not available in every locality”. See section 6.2 for further discussion of broadband provision.

- **Wi-Fi coverage and capacity** was identified as a key challenge by interviewees in Italy and Switzerland. Philippe Devaud observed that a typical problem is that...

“The Wi-Fi coverage does not extend to all parts of the building. To implement BYOD, schools would have to rethink their Wi-Fi coverage”
and that the related additional hardware costs can be very expensive. He added that Gymnase Intercantonal de la Broye (GYB), the school he has been advising, were lucky because they

“could take advantage of a SWISSCOM sponsoring opportunity” and for a small school “without this logistical help, the project would have been too expensive to set up”.

Dario Zucchini in Italy identified a need for access points (see Section 6.1.2.5) able to support

“high crowding” [a high density of concurrent users in a location] “e.g. 128 clients to each access point is normally used on university campuses”,

Dario explains

“without this type of access point, you can’t get even one class onto the net ... In the past, as part of the “Scuola Mia” project, the Ministry supplied top quality office access points that supported the simultaneous connection of a maximum of 20 tablets. With classes of 30 students and an access point of this type you can’t do a lot, because only some users can log on. Access points designed for offices can’t support the kind of traffic a school has ... installing an access point with high crowding every three classes, and estimating 30 students maximum per class, I can be reasonably certain that my wireless network will cope”.

See section 3.3 for further discussion of Wi-Fi planning and implementation.

- **Device management** was a key challenge raised by Väino Tuisk, IT Manager at Pärnu Old Town School in Estonia, as was the device management related challenge of “access control to educational contents” raised by Antonio Santos in Portugal. See section 8 for more discussion of Mobile Device Management.

- **Upgrading access to electricity supply** (i.e. the number of sockets) was noted as a challenge by Philippe Devaud in Switzerland. He advises

“installing switches that can support PoE (Power over Ethernet 31 W) technology... to supply the access points through Ethernet connections... with ... no need to add electrical sockets which can up the costs”.

The Irish Government agree and advise* secondary schools,

“Power over Ethernet (PoE) should be used to power all APs [Access Points]. APs are powered directly via the Cat 6 network cable and avoids the need and associated costs for a separate power socket to power each AP”.

Väino Tuisk in Estonia observed that the need to make arrangements for charging students’ devices can also be challenging.

- **Safeguarding** students from potential online risks is always a concern and a technical challenge for schools in all countries. Dario Zucchini notes that

“An Internet filter is important as it reassures families, kids and teachers”.

It is also of strategic importance as it can

“prevent something [negative and] easily avoidable becoming the sole topic of discussion and argument” about BYOD and the general use of the Internet in school. See section 6.3 for more discussion of safeguarding.

Interviewees also mentioned the related challenges of:

- **Acquiring devices** to be used for BYOD. This is a challenge in Portugal and Antonio Santos identified the problem as a lack of

“financial resources for the educational community [teachers, students, employees and parents] to acquire appropriate devices”.

* Guidance document for the provision of wireless network installations in post primary schools * Department of Education and Skills, Ireland (2016)
See section 8.2 for a discussion of providing device purchase advice to parents.

- **Switching to web based learning materials**, which becomes a more urgent requirement when introducing BYOD and is important, according to Philippe Devaud in Switzerland, to ensure that

  “students can work seamlessly on all their devices, at school and at home”.

This process involves consideration of data protection, which Antonio Santos in Portugal identified as a challenge in addition to

- **“access control to educational contents”**.

Dario Zucchini highlighted a relatively new issue with the increasing use of digital learning materials. He observes that,

“there is no digital book that does not have an associated cloud platform”.

This would not be a problem if all the text books a school wished to adopt came from the same publisher. However, in a particular subject the school may have adopted text books from up to five different publishers.

“Each publisher has their own cloud platform and they each compel schools to carry out the irritating tasks of registering students, creating passwords, etc.”

- **Mismatch between student and teaching staff expectations and knowledge.** Antonio Santos has observed that in many Portuguese schools there are issues arising from the differences between highly motivated students, who have mobile technologies and expect to use these and teaching staff who tend to be more conservative and need to be provided with sufficient continuing professional development to help them adapt.
4. Cloud computing and BYOD

Phillipe Devaud in Switzerland advises that using cloud based services in addition to BYOD enables students “to be both location and device independent”. Commercial organisations also appreciate the way in which combining BYOD with clouds enables them to deliver greater independence to their employees and more flexible services to their customers. An article on the website of Meridian, a US company specialising in managed IT services, observed, “It is no coincidence that the rapid expansion of cloud services and the near ubiquitous presence of mobile devices has occurred virtually simultaneously”. The author added “to me, the two go together like strawberries and cream, peanut butter and jelly, Hot Tamales and popcorn at the movies”.

4.1. What is cloud computing?

Cloud computing involves organisations and individuals using, via the Internet, external shared computing resources rather than, or in addition to, using computing power, applications and data storage resident on their own local servers, computers or devices. The large number of users sharing these resources enables economies of scale to be made which keeps down costs for individual users. The cloud metaphor comes from the fact that most end users of cloud computing resources do not need to know, and indeed do not care, exactly where these are physically located.

Schools may use one or more of three different delivery models for cloud computing the use of which require different levels of expertise to be available in schools, see section 4.6.

4.2. What do these clouds look like?

The physical structure of clouds is distributed networks of computer centres each containing very large numbers of computer servers. Research company Gartner estimate that Amazon is the largest provider of cloud services via their Amazon Web Services (AWS) brand. The online technology news service Data Center Frontier have reported that Amazon has dozens of data centres grouped into regional clusters around the world with each data centre housing between 50,000 and 80,000 servers.

4.3. The benefits of cloud computing

Increasingly, Ministries of Education in Europe are offering guidance for schools on how to effectively implement cloud computing services. A general benefit of cloud computing is that it enables schools to relatively easily and cost effectively provide students, staff and parents with access to school content and services using their own devices from any location with Internet access. Schools are also able to benefit from the economies of scale of sharing server hardware with other organisations and to reduce the administrative burden on school IT staff as this is taken over by or shared with cloud computing providers.

There can be additional cost and resource advantages for schools in using cloud based versions of services needed to manage their Wi-Fi networks and their BYOD policy. These solutions may be developed by schools, if they have the expertise, or can be services that schools subscribe to. Schools can, for example, subscribe to:

- a cloud based WLAN controller solution (see section 6.1.2.5) instead of having a controller resident on the school’s Wi-Fi network and needing to be maintained by school IT Administrators.

5 Lee JC, “Mobility and cloud computing: a natural fit, but enterprise policy needed”, 2014, Meridian
regional centre in Switzerland have compared the cost 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).

A key advantage of cloud computing often cited by commercial companies is its “elasticity”, this means the ease with which the amount and type of computing resources purchased by an organisation can be adjusted to adapt to changing requirements.

Advice to secondary schools from the Irish Government identifies a further advantage of cloud computing saying, “using cloud based services and applications instead of local server based resources can save significant levels of energy” as well as savings on “technical support and associated costs”.

Our Italian interviewee Dario Zucchini commented

“Cloud based services and BYOD devices (with excellent broadband and Wi-Fi) delivers significant economic advantage to the school compared with school owned and managed servers and devices.”

4.4. Cloud computing resource and security considerations

Despite the significant advantages, including cost savings, associated with cloud computing there are some resourcing considerations and security concerns are sometimes expressed.

Security concerns usually relate to free public cloud computing services. An alternative for schools is subscribing to a private cloud service, which provides a secure area, and secure access to it, on a server maintained and managed by a cloud hosting provider.

Some resource implications are obvious. For example, a large number of students connecting to and making prolonged use of cloud based services means greater bandwidth use and increased Wi-Fi network traffic.

Perhaps less obvious is the adoption of cloud computing by suppliers of services to schools. Our Italian interviewee, Dario Zucchini, noted that, “there is no digital book that does not have an associated cloud platform” but schools use books provided by many different publishers and each publisher has their own cloud platform and “they each compel schools to carry out the irritating tasks of registering students, creating passwords, etc.” thereby creating work for IT Administrators or teachers.

Our Portuguese interviewee, António Santos, emphasised that, “using private clouds, and open source tools to develop cloud based services, has cost and efficiency advantages but this does require schools to have staff with the required technical knowledge and experience to do this.

4.5. Cloud deployment models

Many people use public cloud based services that anyone with Internet access can use or subscribe to e.g. Dropbox for storing and sharing files, YouTube for storing and sharing videos. However, companies and schools may feel uncomfortable about locating some of their or their students’ content on public cloud services and handing over responsibility for its security to the service providers.

Alternatively, schools can subscribe to private cloud services. A school can subscribe to its own private cloud, which is a secure area on a server with that server and access to services on it maintained and managed by the cloud hosting provider that owns the server. Private cloud services can be private to a group of schools, plus perhaps organisations they work with e.g. local education authorities or universities, forming a community cloud.

Hybrid cloud models combine two or more of the private, community or public cloud arrangements.

4.4. Cloud computing resource and security considerations

Despite the significant advantages, including cost savings, associated with cloud computing there are some resourcing considerations and security concerns are sometimes expressed.

Security concerns usually relate to free public cloud computing services. An alternative for schools is subscribing to a private cloud service, which provides a secure area, and secure access to it, on a server maintained and managed by a cloud hosting provider.

Some resource implications are obvious. For example, a large number of students connecting to and making prolonged use of cloud based services means greater bandwidth use and increased Wi-Fi network traffic.

Perhaps less obvious is the adoption of cloud computing by suppliers of services to schools. Our Italian interviewee, Dario Zucchini, noted that, “there is no digital book that does not have an associated cloud platform” but schools use books provided by many different publishers and each publisher has their own cloud platform and “they each compel schools to carry out the irritating tasks of registering students, creating passwords, etc.” thereby creating work for IT Administrators or teachers.

Our Portuguese interviewee, António Santos, emphasised that, “using private clouds, and open source tools to develop cloud based services, has cost and efficiency advantages but this does require schools to have staff with the required technical knowledge and experience to do this.

4.5. Cloud deployment models

Many people use public cloud based services that anyone with Internet access can use or subscribe to e.g. Dropbox for storing and sharing files, YouTube for storing and sharing videos. However, companies and schools may feel uncomfortable about locating some of their or their students’ content on public cloud services and handing over responsibility for its security to the service providers.

Alternatively, schools can subscribe to private cloud services. A school can subscribe to its own private cloud, which is a secure area on a server with that server and access to services on it maintained and managed by the cloud hosting provider that owns the server. Private cloud services can be private to a group of schools, plus perhaps organisations they work with e.g. local education authorities or universities, forming a community cloud.

Hybrid cloud models combine two or more of the private, community or public cloud arrangements.

Figure 3: Cloud deployment models
4.6. Cloud services delivery models

Cloud computing allows schools, and other organisations, to effectively outsource elements of their computing services to cloud service providers. The degree of outsourcing varies according to the extent to which schools wish to, or are able to, manage their own services and the availability of cloud based services which meet their needs.

The first column of the diagram in figure 4 illustrates the situation where all services are hosted, maintained and managed within a school or group of schools. However schools may need to, or choose to, purchase one or more of the following services from cloud computing providers:

- **Infrastructure as a Service (IaaS)**
  Organisations subscribing to IaaS are essentially able to build a virtual data centre in the cloud and access many of the technologies and resources of a traditional data centre but they do not need to invest in planning, building, maintaining and managing a physical centre. The Carlos Amarante group of schools in Portugal subscribe to RedHat’s private cloud infrastructure including their Gluserfs distributed file system that stores data across multiple remote servers.

- **Platform as a Service (PaaS)**
  PaaS suppliers provide a platform on which software can be developed and deployed and handle the work of managing servers and network infrastructure, enabling their clients to focus on the application development and business related considerations. The Carlos Amarante group of schools in Portugal subscribe to the Alfresco-in-the-Cloud content management system and open source software (Zimbra Collaboration Suite – ZCS, including an email server and web client and Joomla which enables them to build web sites and online applications) to create cloud based services for their students and staff. Of course, using these open source tools requires technical knowledge and experience and, as Antonio Santos notes,

  "full time IT network support is not available in every school".

- **Software as a Service (SaaS)**
  SaaS is the most familiar form of cloud computing for consumers and educators in which web browsers provide access to software running on cloud servers e.g. Dropbox, Google G Suite for Education, Microsoft Office 365. SaaS has the potential to reduce the cost of software ownership as there is usually little or no need for technical staff to install, manage, and maintain the software. Some SaaS applications may also be free for schools or payment may be by subscription rather than purchasing a software licence.

Figure 4: Cloud services delivery models
5. Some BYOD Examples and key technical lessons learned

BYOD is not a one-size-fits-all solution to the challenges of sourcing and maintaining portable computing devices for school students and facilitating the use of students’ own technology to support teaching and learning. The culture, norms and laws related to the use of mobile devices in schools vary from country to country even within Europe and schools vary enormously according to their size, age, location, history, previous and current use of technology, specialisms and the students and communities they serve. Therefore, many different models of, and approaches to, BYOD exist and advice to schools cannot be one-size-fits-all but rather needs to take into account different types and sizes of schools operating in diverse European countries and cultures with varying levels of technical knowledge and infrastructure. See figure 5 for a few examples of BYOD implementations and lessons learned reported by schools interviewed for this publication.
### Figure 5: BYOD examples and lessons learned

<table>
<thead>
<tr>
<th>SMALL SCHOOLS</th>
<th>Connectivity</th>
<th>Smart phone</th>
<th>Tablet</th>
<th>Notebook/ Laptop</th>
<th>Minimum Spec/Any</th>
<th>Model</th>
<th>Key technical lessons learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle school, Austria</td>
<td>30 Mbps broadband. Small portable routers used to create ad-hoc Wi-Fi hot spots for a small number of devices.</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Any device</td>
<td>Classroom use only via temporary Wi-Fi hot spots.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Technical ingenuity and inexpensive tools means it is possible to experiment with BYOD even when connectivity is very limited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Cloud computing is the future”, the school plans to start using The G Suite for Education (previously called Google Apps for Education) soon.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Regular training for teachers and students is required in skills of computing, safety and security and independent working.</td>
</tr>
<tr>
<td>Primary/ secondary school, Estonia</td>
<td>130 Mbps broadband. Separate Wi-Fi networks for BYOD and school-owned devices.</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Any device</td>
<td>Separate student BYOD Wi-Fi network with limited options and speed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Install cabling all over the buildings to make it easy to add Wi-Fi access points when needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Restrict access to social networking and file sharing sites on school network to save bandwidth.</td>
</tr>
<tr>
<td>Small secondary school, Switzerland</td>
<td>100 Mbps broadband</td>
<td>No</td>
<td>Yes</td>
<td>Minimum spec</td>
<td>BYOD voluntary, students can opt to attend “classic” classes with no technology use.</td>
<td>Installing switches that support PoE (Power over Ethernet 31 W) means you do not need additional electric sockets and therefore saves money and disruption.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Training for teachers is important, limited technical knowledge of some teachers resulted in students being required to use learning materials not compatible with their iOS tablets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cloud based services enable students to be both location and device independent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Do not think the need for printing will disappear completely, “students like to have paper in their hands”, printers should be updated to work over the network and enable printing from all devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“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”.</td>
</tr>
</tbody>
</table>
## BYOD for Schools: Technical advice for school leaders and IT administrators

<table>
<thead>
<tr>
<th>Connectivity</th>
<th>Smart phone</th>
<th>Tablet</th>
<th>Notebook/ Laptop</th>
<th>Minimum Spec/Any</th>
<th>Model</th>
<th>Key technical lessons learned</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LARGE SCHOOLS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large technical secondary school, Italy</td>
<td>1Gbps broadband</td>
<td>Yes, size 5 inch or more</td>
<td>Yes</td>
<td>Yes</td>
<td>Any device</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• It is best to experiment with BYOD over several years gradually increasing the number of students involved 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 802.11ac protocol. Wi-Fi access ‘liberalisation’ followed with all students and staff able to access the network from any device throughout the school.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Installing a mirroring system on all Interactive Whiteboards allows any teacher or student device to project directly onto the board during lessons.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cloud based services and BYOD devices (with excellent broadband and Wi-Fi) deliver significant economic advantage to the school compared with school owned and managed servers and devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• “It is essential to have a centralised authentication (OpenLDAP) and access control (Radius + 802.1X)” to control network access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Instead of blocking bandwidth hungry applications, 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”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Use user profiles with filtering to prevent access to age inappropriate content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Using private clouds, and open source tools to develop cloud based services, has cost and efficiency advantages but requires schools to have staff with technical knowledge and experience.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Make parents/students responsible for their own tech support, IT literate teenagers can help each other and get them to make videos for younger students.</td>
</tr>
<tr>
<td><strong>GROUPS OF SCHOOLS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group of 14 schools, Portugal</td>
<td>1Gbps, minimum 100 Mbps per school</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Any device</td>
<td>BYOD devices used in most classes, if students do not have, or devices are not suitable, they use school tablets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connectivity</th>
<th>Smart phone</th>
<th>Tablet</th>
<th>Notebook/ Laptop</th>
<th>Minimum Spec/Any</th>
<th>Model</th>
<th>Key technical lessons learned</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LARGE SCHOOLS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large technical secondary school, Italy</td>
<td>1Gbps broadband</td>
<td>Yes, size 5 inch or more</td>
<td>Yes</td>
<td>Yes</td>
<td>Any device</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• It is best to experiment with BYOD over several years gradually increasing the number of students involved 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 802.11ac protocol. Wi-Fi access ‘liberalisation’ followed with all students and staff able to access the network from any device throughout the school.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Installing a mirroring system on all Interactive Whiteboards allows any teacher or student device to project directly onto the board during lessons.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cloud based services and BYOD devices (with excellent broadband and Wi-Fi) deliver significant economic advantage to the school compared with school owned and managed servers and devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• “It is essential to have a centralised authentication (OpenLDAP) and access control (Radius + 802.1X)” to control network access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Instead of blocking bandwidth hungry applications, 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”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Use user profiles with filtering to prevent access to age inappropriate content.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Using private clouds, and open source tools to develop cloud based services, has cost and efficiency advantages but requires schools to have staff with technical knowledge and experience.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Make parents/students responsible for their own tech support, IT literate teenagers can help each other and get them to make videos for younger students.</td>
</tr>
</tbody>
</table>
6. Ensuring your school’s technical infrastructure will support BYOD

The decision to introduce BYOD will have the most obvious and most immediate impact on a school’s IT network services and the staff who support that network.

The introduction of 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.

6.1. Terminology and basics

Links to comprehensive online glossaries of technical terms are provided in Section 11. This section includes explanations of some basic concepts and common terms or acronyms to assist understanding of the discussions of infrastructure requirements, Wi-Fi planning and device management in this document. It is also intended to help non-technical school leaders and staff when discussing network requirements with suppliers. Having some grasp of basic concepts and terms is important in order to be able to have informed discussions and to answer some of the key technical questions that will need to be addressed when planning BYOD that are indicated in section 6.2.

6.1.1. Broadband

6.1.1.1. ADSL, VDSL, SDSL and SHDSL broadband connections

ADSL (Asymmetric Digital Subscriber Line) is the cheapest type of broadband connection as it uses ordinary copper phone lines rather than requiring any special line to be installed. Theoretically ADSL can provide up to 24 Mbps download speed with much slower upload speed. However, both speeds depend upon the condition of the wires, the distance to the provider’s location and the amount of interference on the line, so the speeds actually achieved can be very significantly less than the theoretical maximum.

VDSL (Very high bitrate Digital Subscriber Line) makes more efficient use of the copper phone lines and therefore can be up to five times faster for downloads and ten times faster for uploads compared with ADSL. Again the suppliers’ promised up-to speeds are based on ideal conditions and actual speeds achieved are likely to be lower.

SDSL (Symmetric Subscriber Digital Subscriber Line) is generally considered to be a legacy technology and has been succeeded by SHDSL (Symmetrical high-speed digital subscriber line). These are similar to ADSL but offer equal download and upload speeds. This can be an advantage to users, which are usually businesses or organisations rather than households, that need to upload significant amounts of video and other bandwidth hungry content. They also have the advantage of separation of upload and download streams so that downloading is not slowed down by other users.
uploading and vice versa. Unlike ADSL, telephone
traffic cannot share the same wires as data on SDL
or SHDSL.

6.1.1.2. Fibre Optic broadband – Super-fast, Ultra-fast, FTTC, FTTP, etc.

The fastest broadband connections are provided
using fibre optic cable, sometimes referred to as
Super-fast or Ultra-fast Broadband. The term Super-
fast Broadband is frequently used by companies
marketing broadband services but it often just
means broadband products that provide a maximum
download speed greater than 24 Mbps, i.e. faster
than ADSL connections (see 6.1.1).

The price of a broadband connection usually
depends upon the speed of downloading data, for
example when a supplier promises a speed of 30
Mbps they usually mean the maximum download
speed delivered will be 30 Mbps. The speed at which
data can be uploaded is usually substantially less,
especially for domestic customers as it is assumed
that they will want to upload data infrequently.

Theoretically, Ultra-fast Broadband (UFB) has the
potential to deliver up to 1Gbps for both uploads and
downloads but services offering lower download
speeds, and considerably lower upload speeds,
are more commonly offered by ISPs (see 6.1.2.12
Data Transfer Rates for an explanation of Gbps and
Mbps).

Some suppliers now guarantee minimum speeds
as well as promising potential maximum, or “up
to” speeds for fibre connections. Some also offer
services in which speeds are capped to offer a
lower guaranteed minimum speed for a lower price.

Where your school connects to the fibre optic
cable has a significant impact on the speed of the
connection you receive. A variety of four letter
acronyms starting with the letters FTT are used to
describe these connections, the two most common
being FTTP and FTTC.

FTTP - Fibre to the Premises - is a pure fibre-optic
cable connection running from an Internet Service
Provider (ISP) directly to the user’s address.

FTTC- Fibre to the Cabinet – is much more common
and cheaper than FTTP and combines traditional
copper wire cable and fibre optic cable. The
expensive to install fibre optic cable runs to a street
metal cabinet which contain telecommunications
equipment and then more economical copper
wire is used to connect schools (and homes and
businesses) to the cabinet.

FTTP provides the fastest connections, much
faster connections than FTTC, but is much more
expensive both to the supplier and the end users
and many providers only offer FTTP connections to
businesses. However FTTC does deliver very good
fast connections.

6.1.1.3. Symmetrical Cable Broadband

Modern organisations, including educational
establishments, are increasingly finding that modern
methods of working and learning mean they are
using their broadband connections for uploading
data more than they used to. Voice over IP (VoIP e.g.
Skype) services, online collaboration tools, social
media services (e.g. YouTube) and cloud computing
(see section 4) all involve uploading as well as
downloading data. Therefore, broadband services
offering only limited capacity for this will increasingly
seem inadequate.

A potential solution currently being developed
is Symmetrical cable broadband, providing
speeds of 5 to 10Gbps for both downloading and
uploading and sometimes referred to as Full
Duplex. CableLabs, a not-for-profit consortium
responsible for the telecommunications standard
used to provide fibre optic Internet access via a
cable modem (Data Over Cable Service Interface
Specification or DOCSIS), have forecast that the
first Full Duplex trials will take place in 2017.

---

6.1.2. Networks and Wireless networking

6.1.2.1. Local area network (LAN)

A local area network (LAN) is a group of computers and associated devices e.g. printers that share common, traditionally wired, communications links to a server, or servers, and a broadband service. LANs operate in a limited area, typically a building or group of buildings e.g. a school (see figure 6) and can be linked to other LANs to form a Wide Area Network (WAN).

6.1.2.2. Wireless local-area network (WLAN)

A wireless local area network (WLAN) is a computer network that may be standalone or part of a LAN (see figure 6) and links devices using a wireless method within a limited area such as a school, home or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network which usually includes a connection to the Internet.

6.1.2.3. Network name or SSID

An SSID, or Service Set Identifier, is sometimes referred to as a network name and is a unique up to 32 alphanumeric character identifier attached to the header of packets of data sent over a WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

6.1.2.4. School network structure

The structure of school networks varies considerably dependent upon many factors including how recently it was first installed, the size of school, the nature of the building or buildings, the extent to which computers and mobile devices are used, how much cloud computing is used, etc. Figure 6 provides an example of some of the typical devices that may be part of a school network and how these may be connected.

Figure 6: School network example

*Wireless routers are usually controlled by a WLAN controller that may be integrated, a separate device or cloud based
** Wi-Fi Access Points are typically integrated into routers but may be separate devices
6.1.2.5. Routers, hubs, switches, wireless access points and controllers

Some network managers and technicians tend to use the terms router, hub, switch and access point interchangeably, which can be rather confusing, and further confusion can arise as two or more of these technologies may be combined into a single device. These technologies are also sometimes referred to as edge devices, an Edge device being a device that provides an entry point into the core network of an organisation or service provider.

**Routers**, in computing, are networking devices that forward data packets between computer networks. They are located at gateways where two or more networks connect. For example where your school’s local area network (LAN) and your internet service provider (ISP)’s network connect or where your wired LAN connects to your WLAN. Routers read headers attached to data packets and look up forwarding tables to determine the best path for forwarding data.

**A wireless router** is a device that performs the functions of a standard network router and also includes the functionality of a wireless access point (see 6.1.2.5). For most people the most familiar type of wireless router is one in their home that passes data between personal wireless devices and the Internet.

**Hubs** are common connection points for all devices in a network. The weakness of simple hubs is that when they receive data they broadcast it to all devices on the network, not just to the one that requires it. This creates unnecessary traffic on the network and impacts network performance.

**Switches** also forward data packets to devices but they keep a record of the addresses of all the devices connected to them and can therefore send the data directly to just the specific device that needs it. Switches also handle sharing of bandwidth between devices more efficiently than hubs which also helps with network performance.

**A wireless access point** (sometimes called a transceiver) is a piece of networking hardware that allows Wi-Fi compliant devices to connect to a wired network (and via this to the Internet) by receiving and transmitting data. The access point may connect to a router (via a wired network) as a standalone device or it may be a component of a router. Standalone wireless access points are sometimes referred to as “autonomous” or “fat” access points and are less common nowadays. A “thin” access point is one that is managed by a WLAN controller.

**A WLAN controller** provides thin access points with their configuration and also functions as a switch for all the wireless traffic. The use of a controller and “thin” access points is much more scalable than using “fat” access points as this approach saves network administrators the chore of having to manually configure multiple “fat” access points. WLAN controller software, or **virtual WLAN controllers**, can also run on some “thin” access points without the need for a separate, and more expensive, hardware controller. Alternatively, schools can subscribe to a cloud based WLAN controller solution.

**A dual band access point** is one that contains two transmitters, or radios, one operating on the 2.4 MHz frequency band and one operating on the 5MHz frequency band. Dual band access points can be helpful in avoiding interference between access points located near each other. If they are operating on different bands, as well as on different channels within bands, more access points can be installed to support large numbers of users wanting access at the same time in a relatively small area (see section 6.1.2.8 for an explanation of frequency bands and channels).

6.1.2.6. Cat5/Cat5e/Cat6/Cat6a cables and Crosstalk

The quality of the cables used to connect the wired components of a school’s network is important in terms of both the data speeds they can facilitate and how successfully they prevent interference or “crosstalk” between the data they carry. Cat (Category) 5e (Cat 5 enhanced) is currently the most commonly used in new networks; it can support 1000 Mbps speeds and 100 MHz bandwidth and is designed to greatly reduce crosstalk. Cat 5 is made to an older standard, supports 10 to 100 Mbps speeds and up to 100 MHz bandwidth, includes less crosstalk protection and is generally considered to be obsolete. Cat 6 can support 10 Gbps data speeds and 250 MHz bandwidth and includes further improvement of crosstalk reduction. However, Cat 6 can only support 10 Gbps data speeds over a

---

cable length of 164 feet. Cat6A cable can maintain 10 Gbps speeds for 328 feet and exceptionally thick plastic casing helps further reduce crosstalk.

6.1.2.7. Power over Ethernet (PoE)

Power over Ethernet (PoE) is used to supply electricity to networking, audio visual and computing devices connected to a network without the need for power sockets or adaptors. The power supply and the data are transported along the same cable. However, running power supply through a data cable can cause performance and efficiency issues because it heats up the cable. Therefore the category of cable used for PoE is important. An article on the website of the networking and cabling company Belden suggests that, "As much as 20% of the power through the cable can get "lost" in a 24-gauge Category 5e cable, leading to inefficiency" and advise that Cat 6a cables are more efficient and better able to dissipate generated heat. The Irish Government advises schools that “PoE may require additional or new cabling runs. Where this is the case Cat 6a or a higher rated cable should be used to future proof requirements. Using Cat 6a instead of Cat 5, for example, ensures higher data rates can be supported”.

6.1.2.8. Wireless signals, Wi-Fi, Radio Frequency, Bandwidth, Bands and Channels

Wireless signals are electromagnetic, or radio, waves travelling through the air. These waves are extremely useful as they can carry information. Common uses include radio, television, mobile phone, satnav, Wi-Fi and Bluetooth signals.

Radio Frequency (RF) is a measurement representing the rate at which wireless signals vibrate or oscillate. Frequency is measured in Hertz and is the count of how quickly a signal changes every second. Millions of vibrations a second is Megahertz (MHz) and one thousand Megahertz is one Gigahertz. Higher frequencies allow faster transmission of data. This is usually described as having more bandwidth. Higher bandwidth allows files to download and upload faster and the performance of streaming video is much smoother and faster.

Wi-Fi means communication using Radio Frequency (RF) rather than through wires, therefore wireless. Strictly speaking Wi-Fi is a registered trademark of The Wi-Fi Alliance, an international consortium of companies which, since 1997, have followed the Institute of Electrical and Electronics Engineers (IEEE) approach to agree on standards called the IEEE 802.11 protocols. These protocols enable interoperability between products using them, including routers, hubs, switches, access points and Wi-Fi enabled ICT devices like laptops, tablets and smartphones.

Wi-Fi signals operate in two different Frequency Bands, usually referred to as just Bands, dependent upon the frequencies they use. The 2.4GHz frequency band is most commonly used by Wi-Fi technologies. It has the advantage of being able to pass through walls and windows quite well. However, as so many devices use 2.4GHz the signals can interfere with each other. Wi-Fi technologies using the 5GHz frequency band and can achieve higher data transfer speeds. However, the signal cannot pass through walls and windows as well as the 2.4GHz signal. Therefore the range of 5GHz technologies is often shorter.

Frequency bands are divided into channels and devices located near each other and operating in the same channel can interrupt each other. The website of the Commotion community of contributors (Commotion is a free, open-source communication tool that uses wireless devices to create decentralized wireless networks) includes a useful simile for the problem of interference within frequency band channels. They say

---

12 “Guidance document for the provision of wireless network installations in post primary schools” Department of Education and Skills, Ireland (2016)
13 https://commotionwireless.net/docs/cck/networking/learn-wireless-basics/
This situation is exacerbated in the 2.4 GHz band by the fact that channels also overlap (see figure 7). So although the band includes 14 channels only channels 1, 6, and 11 are separated from each other by sufficient frequency that they do not overlap. Also some (typically channels 12, 13 and 14) are reserved for specific non-Wi-Fi communication e.g. television and satellite signals.

There are twenty five 20 MHz wide channels in the 5 GHz frequency band and these do not overlap but the use of some of them is restricted with those that can be used for Wi-Fi being dependent upon regulations enforced in each country.

"Each channel is similar to rooms at a party - if one room is crowded it is hard to carry on a conversation. You can move to the next room, but that might get crowded as well".

Internet Protocol suite (IP suite or TCP/IP) is the conceptual model and set of communications protocols used on the Internet and on most other computer networks. It’s common name of TCP/IP is taken from the original protocols in the suite i.e. the Transmission Control Protocol (TCP) and the Internet Protocol (IP), although many more protocols have since been added. IP specifies the format of packets of data and the addressing scheme for computers to communicate over a network. IP is often compared to a postal system in which someone addresses a package and puts it into the system but there is no direct link between them and the intended recipient. TCP/IP establishes a connection between two devices which then send messages back and forth for a period of time.

There are currently two versions of Internet Protocol operating, IPv4 and an upgraded protocol IPv6. IPv4 is the most widely used protocol connecting devices to the Internet and it can provide just over 4 billion device addresses. However, as the Internet grows unused IPv4 addresses are quickly running out because every device that connects to the Internet requires an address, including computers, tablets, smartphones, game consoles and a rapidly growing number of Internet of Things (IoT) devices.

IPv6, also sometimes called IPng (Internet Protocol next generation) has been designed to provide vastly more addresses. IPv6 also introduces other important improvements to Internet Protocol, including faster data transfer rates and significant security benefits. A large number of Internet Service Providers (ISPs), data centres, cloud services, and software products now support IPv6 and adoption is slowly increasing. According to statistics generated by testing by Google\(^\text{15}\), worldwide adoption of IPv6 grew from 10% at the end of 2016 to approximately 16.5% in July 2017.

---


6.1.2.10. Network Port

A network port is a process-specific, or application-specific, software construct which acts as a communication endpoint and is used by protocols within the Internet Protocol Suite concerned with communicating with external processes and devices. Networking processes or devices use a specific network port, or ports, to transmit and receive data. Each port has a unique number which is assigned and recorded by the Internet Assigned Numbers Authority (IANA). Port numbers 0 to 1023 are well-known numbers that are allocated to standard server processes. For the Internet unencrypted data traffic, identified by the letters HTTP at the beginning of the internet address or URL uses port 80 and encrypted data traffic (HTTPS) uses port 443. Schools may block traffic using other ports in order to prevent circumvention of their safeguarding controls (see Section 7.2 Virtual Private Networks and Section 7.3 Safeguarding).

6.1.2.11. The IEEE 802.11 wireless protocols

The 802.11 wireless standards have been evolving over the years since 1997 with more up-to-date standards supporting enhanced functionality and performance for users of Wi-Fi (see figure 8).

![Figure 8: The IEEE 802.11 wireless protocols](image)

<table>
<thead>
<tr>
<th>Standards</th>
<th>Year Established</th>
<th>Band Frequency</th>
<th>Maximum Data Transfer</th>
<th>Channel Bandwidth</th>
<th>Antenna Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>1999</td>
<td>5 GHz</td>
<td>54 Mbps</td>
<td>20 MHz</td>
<td>1x1 SISO</td>
</tr>
<tr>
<td>802.11b</td>
<td>1999</td>
<td>2.4 GHz</td>
<td>11 Mbps</td>
<td>20 MHz</td>
<td>1x1 SISO</td>
</tr>
<tr>
<td>802.11g</td>
<td>2003</td>
<td>2.4 GHz</td>
<td>54 Mbps</td>
<td>20 MHz</td>
<td>1x1 SISO</td>
</tr>
<tr>
<td>802.11n</td>
<td>2009</td>
<td>2.4 &amp; 5 GHz</td>
<td>600 Mbps</td>
<td>20 &amp; 40 MHz</td>
<td>Up to 4x4 MIMO</td>
</tr>
<tr>
<td>802.11ac</td>
<td>2013</td>
<td>5 GHz</td>
<td>1.3 Gbps</td>
<td>20, 60, 80, 160 MHz</td>
<td>Up to 3x3 SU-MIMO</td>
</tr>
<tr>
<td>Wave 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Up to 4x4 SU-MIMO &amp; MU-MIMO</td>
</tr>
</tbody>
</table>

Clearly, regardless of the bandwidth of a school’s broadband, the speed of connection (the data transfer rate) achievable via the routers, hubs, switches, access points in the school’s network is dependent upon the protocol they use.

When discussing improvements to his school’s wireless network, Dario Zucchini in Italy reported that it had been “updated from this year with a new, even more powerful AC band system [i.e. IEEE 802.11ac] that can potentially handle tens of thousands of users”.

Also, if students’ and teachers’ devices do not support fast protocols they cannot fully benefit from improvements to school broadband and the network. For example, many laptops only support 802.11b or g. However it is possible to upgrade laptops’ Wi-Fi speed by plugging in an inexpensive 802.11ac Wi-Fi dongle. Tablets and smartphones have been designed to take advantage of more recent and faster protocols.

6.1.2.12. Data transfer rates

The speed at which data travels along a broadband or Wi-Fi connection is measured in megabits per second (Mbit/s or Mbps) or increasingly in gigabits per second (Gbit/s or Gbps) and in future Terabits per second (Tbit/s or Tbps) is forecast.

6.1.2.13. SISO, MIMO and MU-MIMO

Early 802.11 standards designated one antenna on a router to transmit and the other single antenna at a device to receive data, this is known as Single Input Single Output (SISO). When multiple devices are using one transmitted signal the speed experienced by each is reduced.

The newer protocols support Multiple Input and Multiple Output (MIMO) i.e. multiple antennae at the transmission point producing multiple streams of data (up to 4) to devices requiring Wi-Fi, thereby increasing performance for each significantly. MU-MIMO (Multi user MIMO) enables up to 8 separate streams.

6.1.2.14. Network monitoring and management tools

As computer networks have become more complex, with more components supporting more users of more fixed and mobile devices in more locations, network managers have required software tools to assist with the necessary tasks of monitoring and managing them. Swiss law requires that schools use Network Monitoring Tools to keep track of all network connections and to store these for 6 months. Philippe Devaud, an IT Adviser in one of Switzerland’s regional ICT Centres, advises schools to subscribe to a cloud based SaaS (software as a service, sometimes called on-demand software) Network Monitoring and Management Tool as these are more cost effective than systems bought to install on school servers.

6.1.3. Security and safeguarding

6.1.3.1. Firewall

A firewall is a network security system that uses rules to control incoming and outgoing network traffic. It acts as a barrier between a trusted network (e.g. a school’s internal network) and an untrusted network (e.g. the Internet) and only traffic that conforms to the definitions in the firewall policy is allowed onto the network with all other traffic being denied. Firewalls can consist of hardware or software or both. A hardware firewall can be purchased as a stand-alone device but they are typically found in broadband routers (see 6.1.2.4).

6.1.3.2. Proxy server

A proxy server also helps to protect a network and its users. It acts as an intermediary between a device and a server from which it is requesting a service. The proxy server may be installed on the same machine as a firewall or may be on a separate server. In companies and schools a proxy server is used to facilitate security, administrative control or caching services and can speed up response times as frequently requested websites are likely to have been previously stored in the proxy server’s cache.

Using a proxy server shields the identity of a device or server it is acting as an intermediary for, as it is the proxy server’s IP address that can be seen by others not the IP address of the device or server itself. This is helpful for schools in guarding against hacking. However, because of this, proxy servers can also be used by technically sophisticated students to circumvent restrictions schools have put in place which limit what students’ IP addresses can access according to the profile created for them.
6.1.3.3. Virtual Private Network (VPN)

Organisations, including schools, often use a Virtual Private Network (VPN) to communicate confidentially over a public network, typically the Internet. For companies it is a way of connecting remote workers to corporate systems or branches to global offices. Schools may use VPNs to connect separate buildings to the school network or to facilitate communication between groups of schools sharing IT facilities. A VPN provides a secure, encrypted “tunnel” for information transmitted between the two locations. Individuals may also use VPN services if they wish to protect their online activity and identity. One reason they may do this might be because they are using free Wi-Fi access in a public place and are concerned that this may not be very secure. Individuals also often use VPNs to circumvent security arrangements that prevent them from accessing services they have not paid for or are not authorised to access. In schools this might include social media, games and entertainment websites that the IT Administrator does not permit students to access.

6.1.3.4. Content/information filtering, blacklists and whitelists

Content or information filtering is the use of a software programme to screen and if necessary exclude from access or availability web pages or e-mails users of the programme consider objectionable (e.g. pornographic, violence or hate-oriented) or a nuisance (e.g. spam emails). In companies and schools content filtering is part of the firewall. In schools filtering software is also often used to prevent access to websites school leaders feel are a distraction or wasteful of school bandwidth e.g. social networking and computer games websites. Parents can also use filtering software on home computers to screen the content their children have access to.

Filtering software can enable users to set up whitelists or blacklists of websites that can or cannot be accessed. Blacklisting allows individual websites that schools do not want students to access to be blocked. Blacklists grow overtime and, to be useful, need to be managed. Dario Zucchini in Italy advises that many schools use a blacklist compiled and kept up-to-date by the University of Toulouse 17 and download updates of newly blacklisted “adult, phishing and other inappropriate sites” every night. Although, it should be noted that the more technically talented students in secondary schools will probably know how to bypass blacklists. Whitelists is a much more extreme, and rather old fashioned, version of content filtering as this prevents access to all websites except those on the whitelist. However whitelisting is much more difficult and time consuming to manage than blacklisting. It requires initial research to identify all the websites all staff and students are likely to wish to access, which is not a trivial task, and then constant updating as access to more sites is requested.

IT staff could also implement whitelists or blacklists of applications which can or cannot run on school devices used by students. It is also possible to blacklist proxy servers or VPNs or to whitelist only specific IP addresses that are authorised to connect to the school network.

6.1.3.5. DNS, DNS filtering and Smart DNS

Every website, like all devices that access the Internet, has a unique IP address and the DNS (Domain Name System) associates these addresses with domain names. When an Internet user types a URL containing a domain name into a search engine the DNS is used to look up the IP address of the website associated with that domain name. DNS is described as being like a telephone directory as it finds the website with a specific IP address number using the domain name.

DNS blocking or filtering is a common and simple method of denying access to specific websites by removing the records associating their names and IP address numbers from the DNS. Therefore, when the name is typed into a browser, the website cannot be found. However, DNS is a distributed network of databases so if users, e.g. students, wish to get around DNS filtering they can do so by using another DNS database to look up the website they wish to access. There are many Smart DNS services available online which enable their users, including students, to do this.

17 https://dsi.ut-capitole.fr/blacklists/index_en.php
6.1.3.6. Traffic/Packet shaping

Traffic shaping, also known as packet shaping, involves regulating network data transfer by delaying the flow of data packets that have been designated as less important or less desired than those of prioritized traffic streams. Regulating flow into a network, i.e. downloading data, may be called bandwidth throttling and regulating flow out of a network, i.e. uploading data, is known as rate limiting. If a school uses traffic shaping tools they can, for example, define how much bandwidth students can use for YouTube so that this remains available for all users but overuse by individual students will not negatively impact on use by teachers for groups of students in classrooms.

6.1.3.7. SSL

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that data passed between the web server and browsers is private. SSL is used by millions of websites to protect their online transactions with their customers and customers recognise when it is being used by the padlock symbol, the word Secure and the letters HTTPS appearing by the website’s URL i.e.

6.1.3.8. 802.1X wireless protocol, Radius and LDAP servers for access control

IEEE 802.1X is generally more secure than the standard IEEE 802.11 protocols which are well documented and well understood by many people and therefore more vulnerable to abuse. It also provides more secure access control for devices connecting to Wi-Fi services as it includes authentication that devices seeking to access the network are authorised to do so, rather than simply requiring that the correct access key is provided. With IEEE 802.1X protocol authentication, a client device (e.g. laptop, tablet or smartphone and sometimes referred to as a ‘supplicant’) that wishes to attach to the network provides credentials (user name and password or digital certificate) to a wireless access point which forwards these credentials to an authentication server (also known as a RADIUS server) for verification. This verification usually involves consulting a database (often via an LDAP - Lightweight Directory Access Protocol - server). If the authentication server determines the credentials are valid, the wireless access point allows the client device access. This process is sometimes described as similar to a visa check at immigration control at an airport before a traveller is allowed to enter a country. Under Swiss law, school systems must include RADIUS/LDAP authentication. Antonio Santos in Portugal agrees

“it is essential to have a centralized authentication (OpenLDAP) and Network access control (Radius + 802.1x)”

to ensure only approved users can get in the school network.

6.1.3.9. WEP, WPA and WPA2

WEP, WPA and WPA2 are encryption algorithms used to secure the information passing along a wireless connection. WEP (Wired Equivalent Privacy) was the original encryption algorithm used by IEEE 802.11 wireless networks and is still used in many domestic and some small business Wi-Fi implementations. However, many years ago a flaw was discovered in WEP which meant it could be cracked relatively easily by people the necessary knowledge and an ordinary laptop. Therefore, an improved approach, WPA (Wi-Fi Protected Access ) was developed. Once again an issue was discovered that meant WPA was not as secure as had been hoped and WPA2 was the solution developed.

There are two types of WPA2 implementation,
6.2. Key questions when planning for BYOD

There are many questions that school leaders should encourage IT staff to investigate when planning to implement BYOD. The diagram in figure 9 includes some key questions that need to be addressed and further discussion can be found in the sections of this document cross referenced.

6.3. 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 1Gbps.

Dario Zucchini, the Digital Coordinator at the Industrial Technical Institute Majorana of Grugliasco (ITIMG) in Turin, Italy advises, “With 100Mbps for a school you can already get started. If this is not enough then you can aggregate the lines using routers, which today can be bought very cheaply, so that you can aggregate, for example, even just 4 lines, each of them with 100Mbps band so that you get 400Mbps… very often [at ITIMG] the net is using 200-300Mbps with 300 desktop PCs and 1,500 wireless users”.

Both Italian and Portuguese experts interviewed recommended 1Gbps bandwidth for large schools or groups of schools.

ITIMG school in Italy are fortunate as they are attached to a university and therefore able to use the GARR ultra-broadband network which provides a 1Gbps fibre optic
BYOD for Schools: Technical advice for school leaders and IT administrators

Carlos Amarante group of schools in Braga, Portugal have a 1Gbps fibre optic connection for the whole group which they share between the 14 buildings. Their Network and Systems infrastructure Manager, António Santos, estimates that individual schools need a minimum of 100 Mbps to support BYOD. Väino Tuisk, IT Manager at Pärnu Old Town School in Estonia, recommends a fibre optic connection and a minimum bandwidth of 130Mbps and the Swiss government recommend “Fibre optic is required to deliver the 100 MB bandwidth necessary for school wide BYOD”.

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. New Middle School Lienz-Nord school in Austria started when just 30Mbps was available (this is now being upgraded to 200Mbps). They enabled occasional, ad-hoc use of students smartphones and tablets by providing teachers with small portable Wi-Fi routers (TP-Link TL-WR710N Wireless N Nano-Router) to use in a classroom to create a Wi-Fi hotspot for these devices to connect to. Although, it seems unlikely that these routers will support concurrent use by more than approximately 5 or 6 devices in a classroom.

Generally the consensus view of European school-based experts interviewed for these guidelines 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 1 Mbps per connected device (e.g. 1000 devices = 1Gbps).

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 (see Section 6.5.3.4. Devices and applications).

NEN- The Education Network in the UK suggested 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 UK have 1Gbps connections”. They also suggested a rule of thumb of 2Mbps per connected device.

It is probable that the demand for bandwidth will continue to increase in most schools in all European countries, with BYOD being one of the factors driving this.

In the USA a 2012 report by the State Educational Technology Directors Association (SETDA) suggested that the amount of bandwidth needed by schools was likely to continue rising by approximately 30% per year. The updated SETDA report published in 2016 references a State of the States report 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 figure 10) 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.

20 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”.
21 “Selecting Broadband Connectivity for Your School”, NEN-The Education Network, 2013
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 staff’s 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.
- The curriculum and the teaching methods employed and the resulting amount of online 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.

Albert Forn, GSMA’s Director of mSchools has noted that “every school in Catalonia has fibre to the door of the school but then there are huge issues to take it beyond that to achieve Wi-Fi that is workable for teachers and students”. He advises that many students in Catalonia bring their own devices into schools and use them informally, in addition to the schools that have “mandated a specific type of device for all students to use in school and at home” (see description of EDUCAT BYOD project in Section 8.2).

### 6.4. 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 fibre optic cables with Virtual Private Networks (VPNs) and/or Virtual Local Area Networks (VLANs) as Carlos Amarante group of schools has done in Portugal. Pärnu Old Town School in Estonia also uses fibre optic cables between buildings. Where there is a line of sight between buildings, Microwave connections, also known as radio bridges, can be an effective and relatively low cost solution.

In some countries FTTC fibre optic connections are now relatively inexpensive and widely available. One effect of this, according to Dario Zucchini in Italy, is that sharing a connection among several buildings is no longer necessary because

“... in the past an old broadband line was so expensive that you had to share it among multiple units, while now with 50 Euro a month you can put [FTTC] into each building. So now there’s no point creating radio bridges between one building and another to get the best connection costs.”
6.5. 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. The Wi-Fi service needs to meet the needs of many users (including students, teachers, administrators and visitors) using diverse devices in a variety of physical locations within and around the school. It has been estimated that “80% of new wireless networks will be obsolete within 18 months due to lack of proper planning.” Planning and design for the medium and long term as well as to address current needs is clearly essential. Many organisations have documented processes for Wi-Fi planning and design, an example is summarised in figure 11.

![Figure 11: Wireless Network Design Process - based on Wireless LAN Professionals Inc. description](image)

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.

António Paulo Santos, Director of computer facilities at the Carlos Amarante group of schools in Braga, Portugal, for example, finds there are, “too many heterogeneous variables and conditions” for automatic planning. He recommends that schools outsource planning and optimisation to external experts only if they do not have available school or local IT experts with the knowledge to undertake this work.

While Dario Zucchini in Italy believes, “It’s never advisable to outsource the planning of your wireless network”, arguing that external experts are knowledgeable about the needs of companies but may not understand the needs of a school. He advises that, “It’s better to set up a [human] network among schools, turning to other schools that have already created this system” for advice and good practice examples. This approach has been successfully trialled in Grugliasco where the Mayor asked ITIMG school to draw on their knowledge and experience to develop the technical specifications necessary to create Wi-Fi networks in all the municipality’s schools.

---

26 Gartner Group quoted in “School wireless network design guide: what you need to know before you deploy a multimedia-grade school wireless network”, Secure Edge Networks 2015.

The Irish Government also advise schools to learn from, if possible by visiting, other schools who have successful Wi-Fi networks. They observe 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”

citing the following reasons:

- The large number of students and associated student devices that need to be supported in relatively small areas.
- The degree of movement among students and staff that takes place in a school is very high, given that in general most users move to a different location in the school every 40 minutes. The timing and simultaneous nature of this movement (i.e. on the bell) does not have an equivalent in office/business/home and, as such, this factor alone makes schools the most demanding environment to support.
- Some ‘industry sector’ solutions are not suitable (e.g. Wi-Fi for a large warehouse may have a wide coverage but be only required to support a small number of users).

Väino Tuisk in Estonia suggests “planner tools are good but it is also good to have cabling all over the buildings to add [more] access points [later] if needed”.

Philippe Devaud reports that ICT centres always advise schools to resort to specialists to set up their Wi-Fi network. Automatic planners rarely work in schools. It is always advisable to hire specialists to set up a powerful network with 100% coverage. Schools that try to go solo end up having to hire specialists most of the time. For new schools they can now count on engineers to set up such connections from the start”.

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

6.5.1. 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.

6.5.2. 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 clients or 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.

Antonio Santos in Portugal told us that the Portuguese government had provided Carlos Amarante group of schools with Cisco access points that support up to 50 users but cost between Euro 1,500 and 2,000. However, when additional access points were needed, budget
constraints meant cheaper devices had to be bought which only support 20 to 25 users each.

Dario Zucchini at ITIMG school in Italy advises, if possible, the use of access points designed for high user density areas that are able to handle up to 128 users per band. He reports that

“I need to put one every three classes. Assuming that in a class I have a maximum of 30 users, there are still a few possible users in this area and this “surplus” is useful because children sometimes arrive with, for example, a mobile phone and a laptop”.

6.5.3. 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:

6.5.3.1. 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.

Another reason why a detailed site survey of school buildings is needed is highlighted in advice to schools from the Irish government, which advises that building structure,

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 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.

Co-Channel Interference (CCI) or Co-Channel Contention (CCC), where Access Points, and devices such as laptops, in close proximity can

---

29 “Guidance document for the provision of wireless network installations in post primary schools” Department of Education and Skills, Ireland (2016)
30 https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Conducting_Site_Surveys_with_MR_Access_Points
31 http://www.tomcarpenter.net/2016/08/24/defining-wi-fi-cci-co-channel-interference-also-called-ccc-co-channel-contention/
impact on each other's communication, can also adversely affect Wi-Fi performance.

Keith R. Parsons of Wireless Lan Professionals has warned that many schools are being advised to adopt a simple approach to Wi-Fi networks of one access point per classroom, without a full explanation of the reasons why this may not always be right for every school. Parsons states that, if after "going through a proper WLAN design process you end up with a series of classrooms, each with a single Access Point", this is not a problem. However, he is concerned about "the trend in our industry of promoting the quick and easy methodology of One Access Point Per Classroom — and without any real design process" and "compounding these bad habits is the practice of not even doing a post-installation validation survey to find how much co-channel interference actually exists, or what other problems might have been created".

6.5.3.2. 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 per second speeds (see Section 6.1.2.11). 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 to ensure that switches used with these can also support gigabit per second 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.

6.5.3.3. 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 (see Section 6.1.2.9). As well as providing more IP addresses than IPv4, IPv6 enables faster data transfer rates and can deliver significant security benefits.

Herman Morgenbesser, European Schoolnet's Future Classroom Lab Lead Ambassador for Austria, reports that "some schools are already working with IPv6" which is "faster and more secure" than IPv4 and "if a school is having a new network installed the supplier will put in IPv6 as it is the state of the art". He advises schools that external suppliers can also upgrade an existing network to IPv6 and that IT Administrators can prepare and save time when upgrading by allocating hardware addresses based on IPv6 even if the schools network is currently IPv4.

IT security company Sophos state that for businesses and other organisations "IPv6 migration is a question of "when," not "if." Services like Google and Facebook are currently available via IPv6 and several large ISPs, telecommunications and web service providers are actively migrating. Mobile operators have pushed for wider IPv6 implementation to support their high-speed networks" and therefore "All businesses should consider their adoption plans, if they haven't already".

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.

6.5.3.4. Devices and applications

What students, teachers 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 what their impact on bandwidth is likely to be. Schools also need to consider what further devices and applications the network may be required to support in the future.

Some companies in the private sector are beginning to talk of Wear Your Own Device (WYOD) as a possible issue to be addressed in the future. 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. Also, because some of the options available for controlling employees’ BYOD devices are not available for wearable devices which may not have much, if any, user-manageable storage. It seems unlikely that WYOD will be a significant issue for schools in the near future. Dario Zuchini observes that they are "tools that communicate short-range, with your smartphone" and "Therefore, they don't interfere with the Wi-Fi".

A number of strategies can be employed to control Bandwidth utilisation by applications, for example:

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

Although 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. Research for EUN’s Interactive Classroom Working Group (ICWG)’s publication “BYOD Bring Your Own Device - A guide for school leaders” found that in Portugal "teachers who are innovative and trying to update their teaching sometimes have their efforts derailed by external actions. For example, the Ministry department responsible for technical aspects of the school’s portal blocking:

- Facebook and YouTube in the mornings, in order to reduce overloading of the service. This was a problem for teachers who had designed learning activities using these tools and whose classes take place in the morning.
- Access to app stores within the school. As a result, the librarian at Carlos Gargaté has to take tablets home to install apps.
- Websites related to computer games, thus preventing 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. António Santos in Portugal has found that it is very effective to "give teachers lots for YouTube for teaching and students little for Facebook".

In this situation, not only do students spend less bandwidth on activity which is probably not directly related to learning, they may also be more discerning about how they use Facebook if they are aware the amount of bandwidth available for it is limited. Bandwidth available for students using specific applications can be capped through the use of traffic, or packet, shaping tools (see Section 6.1.3.6.)

An essential planning tool is a simple table (see figure 12) listing all known and anticipated devices (type and quantity) and the (online) applications expected to be used on these with each assigned a priority rating. The allocation of priorities will be 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.

Priority 1 is those applications which are essential to the running of the school, whilst Priority 3 or 4 might be things which would be nice to have if the network can comfortably support them.

**Figure 12: Device and applications planning**

<table>
<thead>
<tr>
<th>Device</th>
<th>Quantity</th>
<th>Application</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tablet PC – teachers</td>
<td>300</td>
<td>Class register system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Moodle</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Student records system</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet (excluding YouTube and Facebook)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet (YouTube)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet (Facebook)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Skype</td>
<td>2</td>
</tr>
<tr>
<td>Smartphone – teachers</td>
<td>200</td>
<td>Internet</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Moodle</td>
<td>1</td>
</tr>
<tr>
<td>Notebook PC – students</td>
<td>900</td>
<td>Moodle</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>School Email</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet (excluding YouTube and Facebook)</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet (YouTube)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet (Facebook)</td>
<td>4</td>
</tr>
<tr>
<td>etc., etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6.5.3.5. *The performance advantages of filtering*

All schools will wish to apply content filtering to their internet service for child protection reasons (see Section 7.3.1). They will also wish to block adverts and malware which can be inappropriate, a danger to the network and/or wasteful of network resources. A useful side effect of implementing filtering can be more efficient use of bandwidth. Dario Zucchini in Italy has learned that

“When you install a web filter system, even a free one, [there are] various categories available [of things that can be blocked including] malicious and compromised servers... if I put in a good filter system, all of the trash (e.g. phishing and the malware) that very often rides the Internet is eliminated, because it gets filtered at origin, so I don’t download it on my line any more. It could be that with an old broadband line that doesn’t work all that well, by putting in a good filter it will seem to go faster.”
6.6. Rules of Thumb: Technical infrastructure

100 Mbps is minimum bandwidth needed for a small school increasing according to school size, number and use of devices

1 Mbps per connected device (e.g. 1000 devices = 1Gbps) gives a rough estimate of required bandwidth for a large school or a group of schools

Please Note: Rules of thumb are just a starting point when you are thinking of the technology you are likely to need to implement your BYOD strategy. They also help you get started on estimating your likely costs when preparing an initial budget. Be aware, though, that Rules of Thumb if followed without sufficient thought about your school’s particular needs can themselves cause problems. For example, some solution providers use a Rule of Thumb which says schools need one wireless network access point per classroom and in many cases this may be appropriate. However, if the classrooms are close together with flimsy partitions and the access points are using the same channel in the 2.4GHz band, the access points may cause interference for each other.

6.7. Questions to Ask: Technical infrastructure

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. The decision tree in figure 13 suggests some key questions to get you started.

Figure 13: Questions to Ask: infrastructure

- Do you have unlimited data, fibre optic, broadband connection? NO Upgrade before considering BYOD
- Are you maximising bandwidth available to Wi-Fi network end users? YES You are adequately filtering content that can impact bandwidth
- Are you maximising bandwidth available to Wi-Fi network end users? NO Explore the possibility of a BYOD pilot
- Are you maximising bandwidth available to Wi-Fi network end users? YES Consider
- Are you maximising bandwidth available to Wi-Fi network end users? CONSIDER
- Do you have unlimited data, fibre optic, broadband connection? YES
- Do you have plans to increase bandwidth or control demand? YES Is the bandwidth over 100 Mbps? NO
- Do you have plans to increase bandwidth or control demand? NO
- Do you have unlimited data, fibre optic, broadband connection? NO
- Are you maximising bandwidth available to Wi-Fi network end users? CHECK
- Do you have unlimited data, fibre optic, broadband connection? NO
- Are you maximising bandwidth available to Wi-Fi network end users? NO
- Upgrade broadband bandwidth to 1Mbps per device
- Limiting use of bandwidth hungry applications by user role
- Limiting bandwidth available for students for bandwidth hungry applications
- Stopping use of some bandwidth hungry applications
- Limiting number of devices
- Limiting times devices used
- A professional site survey to check positioning of access points and possible sources of interference
- Adding Wi-Fi access points
- Upgrading network protocol, routers, switches and access points
- Using clever students to help police controls and support teachers/students
- Only authenticated users and devices can access your network
- Automatically that no unauthorised access points can be added
- Clever students are not getting around your controls e.g. with proxy servers
7. Risk and security

7.1. 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) reducing the bandwidth available to students, teachers and staff.

7.1.1. 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 wishing to save time and bureaucracy by circumventing network support without fully understanding the possible implications for network services.

7.1.2. User authentication

User access to Wi-Fi networks can be controlled by simply limiting access to users who know the network password. 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 which allows anyone to connect to and start using Wi-Fi without any kind of formalities.

Network security experts advise schools to use a single database of users, and the credentials for each user, 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. The directory service maps the names of network resources to their network addresses. It is a shared information infrastructure for locating, managing, administering and organising network resources and associated items, e.g. volumes, folders, files, printers, users, groups, devices, telephone numbers, etc.

Antonio Santos in Portugal agrees that, “all students must have a profile to access the network” and the services and content they need.

Dario Zucchini in Italy suggests there are a few specific situations in which schools might decide to have completely open access, for example,

Dario believes that in secondary schools it is best for every student to have his or her personal account for accessing the school network. This is empowering for the students and also, “If a problem occurs, you can identify the owner of the [device]” and take appropriate action. This does however

“There are some very enlightened primary schools where the headmaster has said no to passwords... to encourage use [without the barrier of passwords] by both teachers and students”. This approach can work “where around the school there is perhaps a park and the wireless coverage doesn’t extend beyond the territory of the school, then we can allow them not to use a password”. However, Dario warns, if “a school is situated in a closely-packed urban centre... this type of choice risks the inhabitants of the tower blocks around the school being able to browse for free on the school’s line and reducing the bandwidth the school has”.

7.1.3. 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 to be provided (see Section 6.1.3.8 for more information about IEEE 802.1X).

Schools can also blacklist IP addresses that they do not want to access the school network, e.g. the addresses of proxy servers which students may be tempted to use to bypass blocking of specific websites, or whitelist IP addresses so that only devices with these addresses are able to gain access.

7.2. Secure access to school systems and data outside school

Some suppliers and consultants recommend implementing a Virtual Private Network (VPN) to ensure secure access to private school systems and data when students are using BYOD devices for learning outside school. For this reason VPNs are in place in some secondary schools and all upper secondary schools, with or without BYOD, in Switzerland.

However, Dario Zucchini at ITIMG school in Italy warns that "security infrastructures such as VPN need to be managed... It’s unlikely that a lower secondary or primary school can manage a VPN on their own". 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 (see Sections 6.1.2.9 and 6.5.3.3) 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”.

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.

35 “Guidance document for the provision of wireless network installations in post primary schools” Department of Education and Skills, Ireland (2016)

“mean more work for the Digital Coordinator or whoever needs to upload all 500-600 students... when... at the beginning of the year user names and password credentials are given out through a system of centralised authentication”.

“Direct the Wi-Fi provider to adjust Wi-Fi coverage areas to within the external school boundary, and not beyond, especially not into public areas such as nearby roads as this reduces the risk of unauthorised Wi-Fi access”. 

Advice for schools published by the Irish Government
7.3. 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.

7.3.1. Technical safeguarding tools and strategies

Philippe Devaud in Switzerland made the interesting observation, which many educators and researchers seem to agree with, that

“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”.

From a technical point of view there are a variety of 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 (see sections 6.1.3.1, 6.1.3.2 and 6.1.3.4). In some countries, e.g. Switzerland, 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.

Dario Zucchini notes that,

“a web filter is indispensable. We block sites prohibited to minors, to reassure not only the student but also their families and the teacher who can enter the classroom without feeling too worried, knowing that sites prohibited to minors can’t arrive”.

Filtering can include blacklisting specific apps and Philippe Devaud notes that

“a good tool allows a school to block only certain services from a specific app”.

Some schools operate, or subscribe to online Mobile Device Management or Mobile Application Management systems which include content filtering (see section 8.1 for more discussion of MDMS and MAMS).

Google SafeSearch is a useful safeguarding tool. When, in 2015, Google announced their decision to move search results behind SSL encryption (see section 6.1.3.7), saying that encrypting all transactions between search services and their users ensures they cannot easily be accessed by other individuals and organisations, it became necessary for schools to revisit their content filtering arrangements to ensure students were still protected from inappropriate content, links to which could be in search results.

NEN –The Education Network in the UK warned that

“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” and that there is still “a risk of inappropriate search results, including images, being returned and displayed to learners”.

Similarly 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 and some unsuitable content may be still get through.

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. NEN advise that,

---

“In order to perform ‘SSL interception’, schools typically need ... a security certificate...to be deployed to all computers and devices that browse via the school’s filtered internet connection”.

In 2017 1&1, who describe themselves as “a leading worldwide hosting provider” and are used by many small businesses, are encouraging their customers to move to SSL encryption and even initially offering a free SSL certificate to existing customers. 1&1 are advising that

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

Albert Forn, GSMA’s Director of mSchools in Catalonia has noted that

“So some school leaders or IT Administrators want to black out areas of their schools to make sure no Wi-Fi is available there”

to stop students having unsupervised access to the Internet. However, experience suggests that

“It is better to have clear policies that all know and understand, which leads to fewer disciplinary problems”.

7.3.2. Student/staff circumvention of school network controls and safeguards

Many sources have observed that older, more technically literate students, and sometimes staff, will seek to circumvent restrictions put in place by IT Administrators and that this is more likely if more restrictive 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 figure 14).

As noted in the explanation of proxy servers (see section 6.1.3.2), these can be used by students to circumvent school controls, as well as by schools as part of their security arrangements. As long ago as 2009, an article on a BBC website 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”

There are many websites that openly advise students how to get around restrictions on what they can access on the Internet whilst at school. One website says their mission is, “to make the internet more safe, secure, aware and reliable” and to be “regarded as the source for everything related to Internet security, including news worthy of attention, intriguing Internet security concerns, product reviews”; however, they publish articles like “How to Bypass School Internet Restrictions” and “School Proxy to unblock Facebook, MySpace, YouTube and other blocked sites”.

http://www.bbc.co.uk/newsbeat/article/10003579/pupils-bypassing-school-internet-security
7.3.3. Banning mobile phones or banning the use of 3G/4G data connections?

Philippe Devaud reported that in Switzerland, “In most schools, phones are not accepted as school devices. School heads fear students can easily record, film and take pictures of teachers or fellow students. It is more difficult to control this when these devices are connected to the Internet”. This is a common concern raised by schools in many countries.

However, other schools have found that clear acceptable use rules and effective classroom management prevent significant problems from arising. Diana Veskimagi in Estonia observed that, “three years ago [before BYOD was introduced] some parents were worried about phone and tablet use in school”.

Then the school invited parents to digital evenings and showed them with their own devices what their children would be doing. The parents were pleased and there have been no complaints from parents for over two years.

Some schools do not allow students to use mobile phones in school and only allow tablets that are Wi-Fi only. Indeed in some countries, e.g. Portugal, it is illegal for schools to allow students to use mobile phones in school, unless this is for an approved educational project.

The reasoning behind Wi-Fi only devices is usually concern that, if students have a device with a mobile data contract, they will be able to use this to circumvent school controls, access unfiltered Internet content (although European mobile network operators do block the most unsuitable Internet sites).

Staff in most schools in most European countries seem to realise 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.

Regarding students’ use of mobile data in school, it is quite frequently suggested that schools could block the mobile signal. Antônio Paulo Santos, IT teacher and Director of computer facilities at Carlos Amarante group of schools in Portugal, tells us that this would be “easy” but is “illegal”, as it is in most European countries.

Dario Zucchini in Italy suggests that if a large number of students were simultaneously trying to use their mobile data in school, they would be likely to achieve a similar effect, as the mobile network can only support a limited number of concurrent users in a small area. He also observes that,
Encouraging students to choose to use the school Wi-Fi rather than mobile data services is probably a better strategy. If they can use a good Wi-Fi service for no charge they are likely to save their mobile data for when they are somewhere with no Wi-Fi. Dario suggests that this can be achieved by providing a reliable Wi-Fi service with good bandwidth and sensible but not excessively restrictive filtering. Then he says:

“If an illegal jammer were used, these work by disturbing radio communications and therefore also the Wi-Fi [and there would be a] risk of interrupting a public service”.

Sometimes students being able to use their mobile phones can be an advantage to teachers. Diana Veskimägi, Educational Technologist at Pärnu Old Town School in Pärnu, Estonia, told us that all the staff and students are in a temporary building whilst the school is being renovated and:

“the agreement with the students is I give you a free line and you use it properly”.

However, he adds that:

“If field work is done in groups” it can be useful that “there is probably always one student with a good 4G data plan”.

Diana advised that the students are happy to do this and there have never been any complaints by students or parents. Clearly this is an unusual situation and Philippe Devaud commented that:

“In Switzerland it would be unacceptable and against the principle of equity to expect parents to pay for access to school content when [their children] are at school”, i.e. by asking students to use their own mobile data contract, as:

“All materials related to the curriculum should be accessible via the school’s Wi-Fi”.

The students can use their mobile data connection if they have it – but only in the classroom and only when teachers ask them to use their connection to help get around lack of Wi-Fi [also] they can create a hotspot for other students to share.”

“All materials related to the curriculum should be accessible via the school’s Wi-Fi”. 
7.4. A Word to the Wise: Risk and security

Students usually find work arounds when the barriers in place are only Technical.

“No mobiles” policies are almost impossible to enforce in modern secondary schools.

Stopping students using 3G/4G mobile connections and circumventing school Wi-Fi controls is very difficult. Encourage them to choose to use school Wi-Fi instead. If they get good Wi-Fi subject to sensible but not excessive restrictions for no charge they are likely to save their mobile data for places with no Wi-Fi.

7.5. Technical risks planning

School leaders and IT Administrators will be familiar with risk management processes involving drawing up and regularly reviewing a risk register which lists anticipated risks, how serious they are and how likely to occur, together with plans for how they will be avoided or mitigated (see example in figure 15).

Figure 15: Risk Register

<table>
<thead>
<tr>
<th>Risk</th>
<th>Probability</th>
<th>Impact</th>
<th>Avoidance</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>L</td>
</tr>
</tbody>
</table>

Planning for the introduction of BYOD should include a risk planning process, including asking questions about the risks associated with alternative BYOD strategies or models and the school’s capacity to deal with these. Where capacity includes available budget, location and local area infrastructure, the nature and age of buildings, the level of technical staffing and expertise, the school’s culture and school leadership’s risk appetite.

The technical risks planning matrix in figure 16 includes some key risks associated with introducing BYOD and some of the technical options for avoiding or mitigating them. This is not intended to be an exhaustive list of all possible risks and it does not contain non technical strategies (e.g. training, agreed acceptable use policies) for addressing risks which are needed in addition to technical tools and strategies.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Who or what might be harmed</th>
<th>Impact</th>
<th>Prevention and/or mitigation options</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth of school broadband connection insufficient.</td>
<td>Users of school IT systems and the implementation of school BYOD policy</td>
<td>On-line applications very slow; users cannot connect or connection attempts time out. Teachers stop using BYOD devices in teaching.</td>
<td>Upgrade to fastest fibre optic solution available (e.g. 1Gbps FTTC).</td>
<td>Much more bandwidth available.</td>
<td>Cost may exceed budget. May not be available in area. Bandwidth available to end users still low if Wi-Fi equipment not upgraded too.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use firewall, proxy server and/or DNS filtering to block student access to bandwidth hungry websites (i.e. those with downloading and uploading of images, sound, video), or limited times when they can access these, and to keep malware and spam off network.</td>
<td>Less bandwidth use, teachers may like “timewasting” websites blocked, increased bandwidth for legitimate traffic.</td>
<td>Blocked websites not available for teaching. Some students may bypass controls with SmartDNS, VPNs or Proxy Servers and continue using large amounts of bandwidth.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use traffic shaping to cap bandwidth available to user roles and to applications within roles.</td>
<td>Lower bandwidth usage but applications not completely blocked.</td>
<td>Students may use VPNs to bypass caps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Put BYOD students on separate guest-type Wi-Fi network with limited access to the Internet.</td>
<td>Lower bandwidth usage.</td>
<td>Students and their teachers can make only limited use of online resources to support learning.</td>
</tr>
<tr>
<td>Risk</td>
<td>Who or what might be harmed</td>
<td>Impact</td>
<td>Prevention and/or mitigation options</td>
<td>Pros</td>
<td>Cons</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wi-Fi network not able to support increased number of users.</td>
<td>Users of school IT systems and the implementation of school BYOD policy.</td>
<td>Students and teachers finding it slow or impossible to connect to Wi-Fi and/or network slow and unreliable.</td>
<td>Carry out, or commission, site survey to check current coverage, capacity and performance of Wi-Fi network alongside estimating future likely number of devices, where and when these will be used.</td>
<td>Vital input to Wi-Fi planning. Where a large Wi-Fi network is new or being substantially upgraded prospective suppliers can be asked to carry out a site survey as part of the tendering process.</td>
<td>Requires good in-house IT expertise or expenditure on external experts.</td>
</tr>
<tr>
<td>Upgrade Wi-Fi network by adding Access Points and/or upgrading to Access Points that support more devices and/or allow dual channel use.</td>
<td></td>
<td></td>
<td></td>
<td>Increased Wi-Fi network coverage and capacity.</td>
<td>Higher capacity access points are more expensive, disruption during installation, may deliver less than desired improvement if there is radio frequency or co-channel interference.</td>
</tr>
<tr>
<td>After adding additional hardware, carry out a post installation validation survey and adjust positioning to optimise performance.</td>
<td></td>
<td></td>
<td></td>
<td>Improved Wi-Fi network performance.</td>
<td>Some effort and disruption and may be additional cost if external experts are used</td>
</tr>
<tr>
<td>Upgrade to Wi-Fi protocols that support faster data transmission speeds e.g. IEEE 802.11n, IEEE 802.11AC.</td>
<td></td>
<td></td>
<td></td>
<td>Enables achievement of more of the theoretical bandwidth of a high speed broadband connection.</td>
<td>Routers, switches, access points, etc. not compatible with more advanced protocols will need to be replaced. Users with devices that are not compatible will notice less improvement.</td>
</tr>
<tr>
<td>Make sure you know what students and staff are doing and intend to do online with their devices. Review implications for network performance and consider controls listed under broadband bandwidth risk.</td>
<td></td>
<td></td>
<td></td>
<td>Improved monitoring and control of access points, improved performance of Wi-Fi network.</td>
<td>If not currently installed, need to be purchased and installed, involving cost and short term disruption to service.</td>
</tr>
<tr>
<td>Unauthorised Wi-Fi Access points added to school network.</td>
<td>Users of school Wi-Fi network</td>
<td>Reduces network resources available to authorised users, risk of interference with authorised access points.</td>
<td>The network should include a WLAN controller that monitors access points and will detect any new ones added and not registered.</td>
<td>Improved monitoring and control of access points, improved performance of Wi-Fi network.</td>
<td>If not currently installed, need to be purchased and installed, involving cost and short term disruption to service.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td><strong>Who or what might be harmed</strong></td>
<td><strong>Impact</strong></td>
<td><strong>Prevention and/or mitigation options</strong></td>
<td><strong>Pros</strong></td>
<td><strong>Cons</strong></td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------</td>
<td>------------</td>
<td>----------------------------------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Network accessed by unauthorised users.</td>
<td>Users of school Wi-Fi network and school network and data.</td>
<td>Reduces network resources available to authorised users. May introduce malware or enable unauthorised access to confidential information.</td>
<td>Require all students to enter id and password to access the network and set up profiles for students defining what they are able to access.</td>
<td>Reduces risk of unauthorised users on the network. Easier to identify any authorised user behaving incorrectly on the network.</td>
<td>Time and effort required each year to set up profiles for all students.</td>
</tr>
<tr>
<td>Students may access age inappropriate material or unsafe websites while in school.</td>
<td>Students, the reputation of the school and implementation of school BYOD policy.</td>
<td>Students and parents could be upset, students could be harmed, the school could be in breach of their safeguarding responsibilities and might even be sued.</td>
<td>Use firewall, proxy server, DNS filtering and content filtering - possibly including subscribing to a blacklist maintained on behalf of schools - to block undesirable websites and applications.</td>
<td>Reduces risk of students accessing inappropriate or unauthorised websites.</td>
<td>Requires IT expertise but some of these methods will already be in use in schools prior to BYOD.</td>
</tr>
<tr>
<td>Students accessing age inappropriate material from online services using SSL encryption e.g. Google, Facebook, YouTube.</td>
<td>Students, the reputation of the school and implementation of school BYOD policy.</td>
<td>Students and parents could be upset, students could be harmed, the school could be in breach of their safeguarding responsibilities and might even be sued.</td>
<td>Use Google SafeSearch, YouTube Kids iOS and Android apps and Restricted Search option on YouTube website.</td>
<td>Most inappropriate material will be blocked.</td>
<td>Some inappropriate material may not be stopped by these tools.</td>
</tr>
<tr>
<td>Students using technical tools to bypass IT Administrator restrictions.</td>
<td>Users of school IT systems, students, the reputation of the school.</td>
<td>Bandwidth available for other users could be reduced, students may be accessing age inappropriate material.</td>
<td>Blacklist IP addresses of VPNs and proxy servers being used by students and block ports typically used by VPNs.</td>
<td>Stops students using specific proxy servers and VPNs to bypass school controls.</td>
<td>The risk is unlikely to be permanently removed if technically literate students switch to alternative tools.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Involve the students with the best technical skills in this area in helping to police the network.</td>
<td>The students know how they would try to get around controls. Recognises their skills, encourages them to use them responsibly and enhances their CV.</td>
<td>Need to identify the best students to involve and get school leadership agreement to the incentives given.</td>
</tr>
</tbody>
</table>
8. Device and Application Management

A key decision that needs to be made when developing a BYOD strategy 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.

8.1. 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 as they would other network resources. 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. MDMS can save IT staff a great deal of time carrying out routine device administration and maintenance. It is also possible to monitor 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.

This is clearly advantageous for companies who issue mobile devices to employees and/or allow employees to use their own devices on the company network. MDMS simplifies providing maintenance and technical support and ensures that company data and the company network are protected in a similar way to when employees use desktop computers in the office.

MDMS is also 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.

The Irish Government, in published advice to secondary schools⁴⁰, observe that MDMS, “are fast becoming important tools to manage mobile devices in schools” and “can assist in managing security risks”.

Philippe Devaud comments that

“managing 1000 devices without such a solution is a logistical nightmare and will cost much more in work hours”

than implementing an MDMS system. Also Swiss law requires a school operating BYOD to implement an MDMS able to track which devices are connected to which content and to store this information for six months.

In Switzerland Philippe Devaud advised that school

“MDMS systems are very useful for Over The Air distribution of textbook and software licence keys and management of these keys”, the school can “distribute all keys in one click [and] deactivate keys at the end of the school year”.

He also says that,

“Roaming management [that is] going from one network to the other” makes it possible “to configure to block devices in certain circumstances [which can be used to] block access to the network during exam periods”.

However, whilst school IT support staff may find MDMS very helpful, in many countries the use of MDMS in schools is controversial, particularly where the BYOD model is that students may bring in and use in school their personal mobile devices. Concerns have been raised about systems which enable schools to monitor what students’ do online outside school and to effectively monitor where they go. Antonio Santos of Carlos Amarante group of schools in

---

⁴⁰ “Guidance document for the provision of wireless network installations in post primary schools” Department of Education and Skills, Ireland (2016)
Portugal comments,

“MDMS is dangerous if it is tracking what students are doing, parents may not like their children being tracked”.

There can also be problems with monitoring students’ use of devices within school. An article providing legal advice to school administrators in the USA observed,

“When schools own the devices being used in a 1-to-1 program, they have an increased ability to monitor the activities on those devices and search the digital contents to investigate individualized suspicion of a disciplinary incident. Searching an iPad that a student is borrowing is like searching a locker (both are owned by the school), while searching a student-owned iPad is more like searching a purse that is clearly a student’s private property. Thus, districts that have BYOD policies permitting student- or parent-owned devices in school have a much harder time searching or seizing those devices after suspicious activities”

and advised that there have been court cases as a result of schools monitoring students’ devices and then taking disciplinary action.

Many suppliers of network related products and services advise schools that MDMS is “very important” or “vital” and sometimes, in addition to emphasising the efficiency gains for IT support staff, warn about child safeguarding issues e.g.

“Without a suitable mobile device management software tailored for education in place, access to inappropriate content … can occur unchecked. The same is true of playing online games and accessing social media at the expense of studying and maintaining student attention”

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 (see Section 8.1). Also, good teachers will be aware of classroom management strategies that focus on the challenge of maintaining students’ attention and encouraging them to focus on educational tasks and schools may decide they do not need technical solutions to address these challenges.

Another important consideration regarding the use of MDMS with student owned devices is that their personal data on these needs to be protected. For example, if the school remotely updates software on the student’s device, personal data must not be lost. Managing secure access to school data and protecting students’ personal data means increased workload and responsibilities for school IT support staff.

Dario Zucchini explains one potential practical problem with MDMS and BYOD as,

“I must oblige users to install a programme of my choice, in order to control his or her personal terminal [but] the student can decide ‘I don’t want this app that remotely controls the tablet … I’m going to uninstall it [and] As soon as the student has uninstalled the remote-control app, you’ve already lost control from a distance”.

Pärnu Old Town School in Estonia have two separate Wi-Fi networks, one for student’s BYOD devices and one for school owned devices and teachers’ devices. MDMS is only used with school owned devices. However, the Wi-Fi network for BYOD devices only provides access to a limited service.

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 employees’ devices, whilst delivering some of the advantages of MDMS around protecting corporate data and systems.

Mobile Application Management systems (MAMS) provides the IT staff with the ability 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 if an employee or student leaves the organisation. This is all done without the need to install client software on mobile devices or to interfere with any personal applications and

---

42 https://www.imperosoftware.co.uk/byod-mobile-device-management-software/
 Philippe Devaud has observed that, “Such tools are relevant in tablet or laptop schools where the school manages all devices as well as the distribution of software and digital content”; however, “From upper secondary schools, students [in Switzerland] have to manage their devices by themselves and are responsible for downloading the necessary tools” and “most content is distributed via web interfaces anyway”.

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. The regional ICT centre fri-tic have compared the cost, for a school of 1000 students, about 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 IT departments supporting corporate BYOD are implementing “containerisation”, which enables separation of corporate apps and data from employee apps and data on employees’ BYOD devices and the IT department then only has control of 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.

8.2. 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, initiated by Wolverhampton local education authority in the UK, involved working with device manufacturers on the specification for netbooks to be purchased by parents to support teaching and learning in their schools. Other local or regional authorities in many countries have recommended, or purchased for students, specific consumer ICT devices e.g. Asus netbooks, 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 notebooks, 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. Acer Android tablets and Acer Chromebooks have also been chosen by parents in some schools.

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 been offered: an Acer extended warranty; service support in the local language (Catalan); dedicated service phone line support which can be used by parents, schools or solution integrators to access help quickly if problems arise and a fast repair service.

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 (see section 6.1 Terminology and Basics), to achieve faster network connections (the supplier claims three times faster) than achieved by devices using the 802.11n protocol.
8.3. Preparation, maintenance and technical support for BYOD devices

8.3.1. 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 could be carried out at home by students. Dario Zucchini in Italy says,

“we must say to the kids to download updates at home and not at school, because if there are 1,000 tablets per day doing updates every school day, then even 100MB [broadband] won’t be enough. The policy must be to say: bring terminals to school without viruses and without updates to do, so we can use the broadband for education only”.

8.3.2. Maintenance of BYOD devices

There are a number of possible alternative approaches to maintenance of students’ devices that include:

- simply making this the responsibility of the student;
- and/or the school, or local education authority, negotiating 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 is responsible for device maintenance.

In Switzerland, Philippe Devaud advises,

“It is necessary to have a list of apps shared among all the teachers, which must be few but good so that we can say to families: we use computers in the classroom to do these tasks. The books adopted are these, and the apps to be installed are these, so if you’re bringing a tablet to school then please install these apps so that it can be used in the classroom”.

Dario Zucchini advises,

“as much as possible, get the students and their families to service their tablets properly, then if you get a student who has problems with one, there will also be some clever student in the class who can fix it. This helps us too, and there’s also a little bit of peer education in this way. In every class, there’s always some clever kid who can help the teacher in solving technical problems and you must also remember to give good marks to these kids who are good at IT”.

“from upper secondary school, students have to manage their devices by themselves and are responsible for downloading the necessary tools, most content is distributed via web interfaces”.
8.3.3. Technical support for BYOD students

Interviewees were asked what arrangements they recommend schools should make to provide technical support to 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. However, 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.

Dario Zucchini in Italy says,

“If the school provides a computer, families expect the school to guarantee assistance. If instead it’s the students who bring devices to school this reduces the management burden. There’s a lack of funds and resources, and to allocate a teacher to be a system engineer at the disposal of the kids is a mistake. The teacher must teach the children through the devices and not take care of these”.

At Pärnu Old Town School in Estonia students can bring in any smartphone or tablet but the school does not provide any technical support and according to the Educational Technologist Diana Veskimagi

“They don’t need any support usually, mostly they sort it out themselves or with friends”.

Philippe Devaud in Switzerland suggests,

“Using students as helpers can be both rewarding for the students and cheaper than hiring technical staff. Two students can be trained in each class to serve as tech support”.

However,

“It is important to define procedures: how long do the student helpers try to solve problems? When do they call the professionals? Is there a helpdesk on site, etc.?”. 

Antonio Santos, in Portugal reports that

“There is a shortage of trained staff” and “It’s a miracle if you have a teacher who understands networks”.

He runs courses for IT students who then provide support for themselves and their peers but says that,

“parents and students need to understand they do their own tech support”.

Adelina Moura, a teacher and researcher at the school includes information literacy in her classes, including what students can and cannot do and what problems may arise. She notes that,

“The teenagers are IT literate and can help each other and they sometimes create videos to help the younger students”.

Adelina is the co-ordinator of a European club and students’ videos are shared via a club blog with other countries and schools.

8.4. A Word to the Wise: Maintenance and Support

Avoid wasting school bandwidth, and time, on set up and maintenance tasks which can be carried out at home by students. Have an agreement that they bring to school a device with the required software/apps installed and the latest updates applied; with no viruses or malware and with the batteries fully charged.

Use, and reward, technically adept students to assist their peers, teachers and the IT administrator.
9. Sources of further information

Some useful and relevant further reading can be found in the following sources:

- The Education Network (NEN), who describe themselves as, “A group of not for profit and public sector regional organisations working across the UK to bring high quality, future proof broadband services, independent ICT advice and online educational content to schools, academies and other educational settings”, have published useful advice on a number of technical issues related to BYOD including: selecting broadband connectivity, protecting the school network, eSecurity, cloud computing, BYOD, and “Using Consumer IT Devices in Schools” 43.

- Cisco’s “Wireless LAN Design Guide for High Density Client Environments in Higher Education”44 is intended for wireless network design engineers responsible for designing, deploying, and maintaining Wi-Fi networks within high-density environments in universities or colleges. Where high-density means any environment with a large concentration of users, such as a classroom, lecture hall, or auditorium where the users are connected wirelessly, sharing applications and using other network services individually. The guide provides engineering guidelines and practical techniques for designing, planning, and implementing a wireless LAN (WLAN). However, it does assume the reader already has knowledge of Cisco networking concepts, WLAN technology fundamentals and Cisco Unified Wireless Network (CUWN) features and configurations. Cisco Meraki’s website also contains a useful documentation section including general articles and information regarding best practices and wireless networking fundamentals45.


- “School wireless network design guide what you need to know before you deploy a multimedia-grade school wireless network”47, Secure Edge Networks, 2015


---

45 https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices
10. Acronyms

The following acronyms are used in this document, they are explained in the text and further explanation can be found by consulting the glossaries referenced in Section 11.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>3rd Generation</td>
</tr>
<tr>
<td>4G</td>
<td>4th Generation</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>BYOT</td>
<td>Bring Your Own Technology</td>
</tr>
<tr>
<td>Cat5</td>
<td>Category 5</td>
</tr>
<tr>
<td>Cat6</td>
<td>Category 6</td>
</tr>
<tr>
<td>CCC</td>
<td>Co-Channel Contention</td>
</tr>
<tr>
<td>CCI</td>
<td>Co-Channel Interference</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>FTTC</td>
<td>Fibre To The Cabinet</td>
</tr>
<tr>
<td>FTTP</td>
<td>Fibre To The Premises</td>
</tr>
<tr>
<td>Gb</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>Gbps</td>
<td>Gigabits Per Second</td>
</tr>
<tr>
<td>GHz</td>
<td>Gigahertz</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol - Secure</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute Of Electrical And Electronics Engineers</td>
</tr>
<tr>
<td>IPI</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPng</td>
<td>Internet Protocol Next Generation</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol Version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MAMS</td>
<td>Mobile Application Management System</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits Per Second</td>
</tr>
<tr>
<td>MDMS</td>
<td>Mobile Device Management System</td>
</tr>
<tr>
<td>MHz</td>
<td>Megahertz</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input And Multiple Output</td>
</tr>
<tr>
<td>MU-MIMO</td>
<td>Multi User MIMO</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air Distribution</td>
</tr>
<tr>
<td>PoE</td>
<td>Power Over Ethernet</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role Based Access Control</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software As A Service</td>
</tr>
<tr>
<td>SISO</td>
<td>Single Input Single Output</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>Tbps</td>
<td>Terabits Per Second</td>
</tr>
<tr>
<td>UFB</td>
<td>Ultra-Fast Broadband</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VDSL</td>
<td>Very High Bitrate Digital Subscriber Line</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WYOD</td>
<td>Wear Your Own Device</td>
</tr>
</tbody>
</table>
11. Glossaries of technical terms

The following excellent online glossaries provide explanations of relevant technical terms and are kept up-to-date by their authors:

- **Webopedia** ([www.webopedia.com](http://www.webopedia.com)) is an online tech dictionary for IT professionals, educators and students, providing easy-to-understand, frequently updated definitions of words, phrases and abbreviations related to computing and information technology. Webopedia say their definitions come from “standards bodies, leading technology companies, universities, professional online technical publications, white papers and professionals working in the field” and definitions are never based on just one source. Webopedia also provides in-depth articles, study guides and links to sources of further information.

- **Watis.com** ([http://whatis.techtarget.com](http://whatis.techtarget.com)) Watis.com describes itself as “a reference and self-education tool about information technology. The site provides readers with definitions for over 10,000 terms and over 1,000 fast references, cheat sheets and quizzes. Watis.com is updated each weekday and is used primarily by information technology (IT) and business professionals. The site’s mission is to help IT pros and the business people they work with understand each other’s highly specialized languages. The definitions are known for explaining technical terms and business concepts clearly and concisely. Watis.com was created by IBM technical writer Lowell Thing in the early days of the Internet. In 1999, TechTarget acquired the site and for the last decade site content has been researched and written by editorial director Margaret Rouse and content editor Ivy Wigmore with the assistance of contributors and technical experts from over 60 countries”.

- **Gartner IT Glossary** ([www.gartner.com/it-glossary]) Gartner describe their glossary as “IT Glossary is your trusted guide to exploring technology terms and definitions, from the world’s leading IT research and advisory company”.

- **Techopedia** ([www.techopedia.com/dictionary]) Techopedia describe their aim as “At Techopedia”, we aim to provide insight and inspiration to IT professionals, technology decision-makers and anyone else who is proud to be called a “geek”. From defining complex tech jargon in our dictionary, to exploring the latest trend in our articles or providing in-depth coverage of a topic in our tutorials, our goal is to help you better understand technology - and, we hope, make better decisions as a result”.

12. Acknowledgements

The valuable contributions and assistance of the following are acknowledged and greatly appreciated.

**Interviewees**
Georg Koeck, IT Administrator and eLearning Lecturer at New Middle School Lienz-Nord, Austria  
Hermann Morgenbesser, Future Classroom Lab Lead Ambassador for Austria  
Vaino Tuisk, IT Manager at Pärnu Old Town School, Estonia  
Diana Veskimägi, Educational Technologist, Pärnu Old Town School, Estonia  
**Tom Lonergan, Professional Development Service for Teachers (PDST), Ireland**  
Dario Zucchi, Digital Coordinator, Industrial Technical Institute Majorana of Grugliasco (ITIMG), Turin, Italy  
**Antonio Santos, IT Director, Carlos Amarante group of schools, Portugal**  
**Adelina Moura, Teacher and Researcher, Carlos Amarante group of schools, Portugal**  
Philippe Devaud, Information Technology Adviser, Regional ICT centre Fri-tic, Switzerland

**Industry contributors**
Anna Artemyeva, EMEA Education Program Manager, Acer  
Albert Forn, Director of mSchools, GSMA  
**Beryl Furlong, Wriggle Education, Ireland**

**European Schoolnet Interactive Classroom Working Group members**
Karl Lehner, Austria  
**Leonardo Tosi, Italy**  
Ene Koitla, Estonia  
**Fernando Franco, Portugal**  
Madeleine Murray, Ireland  
**Stephanie Burton, Switzerland**
Bring Your Own Device for Schools

Technical advice for school leaders and IT administrators

The publication, “BYOD for Schools: Technical advice for school leaders and IT Administrators”, has been developed 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.