Going beyond your existing information technology infrastructure

How schools can stay top of class when it comes to providing the most efficient learning environment for pupils

D-Link®

Contents

Network Access; Furtureproofing your network infrastructure; Policy decisions when setting a strategy

1. Introduction

Technology has moved on at such a pace in recent years and children have become so technologically-savvy that ICT is no longer a lesson to be taught, but a tool to use for the teaching of other subjects.

But the wholesale use of computers, laptops, tablets, mobile devices and smartphones in educational establishments brings a brand new set of challenges for primary and secondary schools to overcome in order to successfully embrace this increasingly commonplace way of learning.

This guidance paper for heads, principals, decision-makers and ICT professionals is intended to explain how the use of computers and mobile devices continues to revolutionise our classrooms and what schools need to consider with regard to their IT infrastructure to make such a policy work.

Although all schools are obviously different, there are a number of fundamental factors that deserve due consideration before key decisions are made – faster wireless and access points within a Managed Wireless Network (MWN), the advent of 1:1 learning, strategic policy decisions, network policy integration with current devices that may need to be taken as part of a Mobile Device Management (MDM) masterplan and the potential monetisation of facilities through guests, scheduled access and out-of-hours users.

You will probably find the key question that needs answering is whether networks can cope with an influx of devices and what upgrades, improvements or complete rebuilds would be necessary to future-proof any systems installed or considered. Conventional wisdom would suggest that implementing and managing networks to make the school teaching and learning environment effective and enhanced, and the computer system easier and flexible to maintain are the crucial aspects of any ICT decisions.

Sarah-Jane Francis, ICT specialist at the 425-pupil Wood End Academy for 7 to 11-year-olds in Greenford, West London and part of the Ealing local education authority, said: “Computer capability is seen as a core skill to be learnt at school along with numeracy and literacy. We have an ICT suite equipped with computers, linked to the internet as well as class sets of wireless enabled laptop computers and tablets.

"We are a 21st century school with a specialist room for Information Technology and a computer for every child in the class which is linked to the Internet. We have an iBoard Touch Interactive Whiteboard in every classroom. The children have lessons in computer skills and put those skills to use to enhance their learning in other curriculum areas."

While this may sound exceptionally complicated, it should be remembered that there are highly skilled ICT experts with many years of experience who are able to steer educational establishments in the right direction to [achieve] the best possible outcome with regards to enabling teachers and students to [achieve] goals.

Rarely do two schools require exactly the same solution and bespoke systems are generally the order of the day, but the underlying principles often remain the same – go for a good set-up, don't cut corners on funding only to regret it later, and, most importantly, carefully consider what is required and take advice (from partner organisations, other schools, users, experts and even students) on how to achieve that outcome.

Nigel Pressnell, headteacher at The Arnewood School, a 1,200-pupil academy for 11 to 19-year-olds in New Milton, Hampshire, says his school has a long-established IT policy with a number of upgrades over the years. The school is moving from laptops to tablets as the preferred mobile device.

"Our 'virtual learning environment' allows teachers to set homework and tasks online, remain in contact with pupils when necessary and is the preferred way of working for the sixth form."

You may feel that the correct approach is to take a long-term view with the initial steps foundations and building blocks for the future embracement of a flexible, lifelong learning system.

Any new system represents a major change for both educators and learners with the potentially different relationship between school and student something that needs taking into account.

In short, it's a big subject with far-reaching consequences and decisions need careful consideration. This paper will hopefully help you to approach these matters fully armed with relevant and necessary information.

2. Schools' checklist

Whether you are installing a new information technology infrastructure for your school or updating a current environment, here is a summary checklist covering many of the issues that need to be addressed:

- ☐ Decide exactly what you want to achieve from your network by reviewing current network diagram and proposed plans.
- ☐ Make informed decisions after consulting with other schools who have been through the same process and the school has reviewed the survey document for a site visit. Call in the professionals to guide you through complicated IT purchases
- ☐ Invest in the best possible and most robust network from the start
- ☐ Do your research to get the initial infrastructure groundwork right, design the network to best match your requirements and what the network will do for you on a return in investment
- ☐ Leave teachers to teach and not have to become IT experts
- ☐ Allow ample time for training of staff
- ☐ Consider installing a Mobile Device Management system to centrally control and monitor network use and mobile integration for policy rights.
- ☐ Have processes in place to ensure there is no digital divide between pupils
- ☐ Formulate a workable and fair policy regarding the use of your network, mobile devices and internet access
- ☐ Fully engage stakeholders – teachers, governors parents – to ensure buy-in to policy decisions
- ☐ Invest in devices that match the requirement, don't use over-specified products that have technical features that will not be used.
- ☐ Futureproof your network as far as possible to accommodate growth, always consider scalability and expansion.
- ☐ Remain flexible, anticipate challenges

3. Managed Wireless Network (MWN)

i) Faster wireless

It is imperative that the wi-fi network is reliable, secure and provides a long-term investment for the school. Thinking only of a short-term return is not recommended. What works well today may not perform adequately in future when more mobile devices may be needed, learning structures change, greater emphasis is placed on downloading material quickly, or technology continues to evolve.

Investment in the best possible network is essential – it is not an option to think otherwise. Pupils in lessons using devices and also recording and uploading to the network at the same time will undoubtedly need huge capacity, especially if there are, say, 30 students in 10 classrooms, meaning 300 youngsters simultaneously wanting network access. Students carrying two or three devices running multiple applications, each using network resources, will compound these traffic issues.

Former teacher Steve Hazle, now an integral part of ICT services, solutions and support specialists Levett Consultancy, who deal extensively with schools nationwide and are based in Ongar, Essex, said: **"It's all about the infrastructure. You have got to get the groundwork right at the start. It is absolutely key to know what you want to be achieved and ensure your set-up is capable of delivering this and is able to grow with you."**

While the advent of BYOD means there may possibly be less need for institutional capital expenditure on computer equipment, it should be remembered that providing better wi-fi aligned with increased network management costs and overheads could well counterbalance any savings. Thus the primary driver of this process should be viewed as necessary improvements designed to facilitate better learning, rather than an opportunity to cut costs.

Wireless is a shared environment – wired is not – and anyone can use it. Ensuring that the sharing process allows full accessibility to all users is one of the obstacles that need to be overcome.

Craig Judd, IT Network Manager at the 1,250-capacity Parkstone Grammar School, an all-girls secondary academy school in Poole, Dorset, says: **"We utilise a system using both the faster 802.11ac wireless networking standard and the legacy 802.11n in both 2.4ghz and 5ghz. We have pervasive, fair coverage across the campus and pretty much access for all anywhere."**

Hazle adds: **"Teachers don't want to have to worry about the wireless network and technicalities other than just turning it on and knowing it works for a class of 30 pupils. It is simply a modern tool to be used and regarded in a similar way to a blackboard of old – it's utilised without a second thought."**

Pressnell says:

"IT purchases are fraught with danger from the consumer's point of view. Taking on a well-qualified consultancy to guide you through the process is imperative – as is the robustness of the after-sales service. The technology needs to work first time you take it out of the box. Teachers are not technicians and neither would I want them to be – anything that IT experts can do to make the whole process as seamless as possible is welcomed."

ii) Wireless AC Standard

The newest generation of Wi-Fi signalling in use is 802.11ac that utilises dual band wireless technology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz.

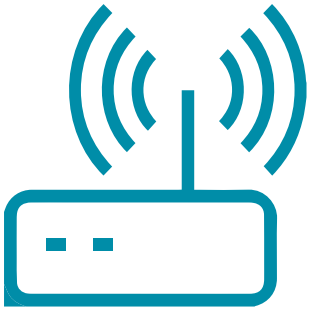
iii) 2.4ghz v 5ghz

One of the questions that will need answering is whether you utilise 2.4ghz or 5ghz. Put simply, they are just different frequencies with different capabilities, but it should be remembered that virtually all devices with wireless have 2.4ghz as standard and not all devices can access 5ghz. The main differences are bandwidth and range. The 5ghz gives faster data rates, but usually over shorter distances, whereas 2.4ghz may well perform more slowly but can cover a greater distance. It may be helpful to also explain some of the more subtle differences to provide clarity.

It is generally recognised that higher frequency wireless signals such as 5ghz perform less well outside the classroom, being unable to pass through walls and floors, meaning data will not travel far successfully. Lower frequency wireless signals such as 2.4ghz are better at this and so have a greater range, say, from classroom to classroom.

Bandwidth is a range of frequencies within a given band, in particular that used for transmitting a signal or data. Thus with a higher bandwidth such as 5ghz, files can be uploaded or downloaded faster than when using 2.4ghz – which may be deemed important, particularly if streaming video or utilising large files is a regular occurrence.

It was mentioned previously that most devices only use 2.4ghz. This means that overcrowding of



channels is inevitable when multiple users all use 'radio space' at the same time. 2.4ghz has 11 channels, but only three don't overlap. Thus if there are just three access points it works at full speed, if there are more it is slower - whereas 5ghz has 23 non-overlapping channels that don't overlap in a wide range of frequencies.

Therefore, overcrowding of channels can cause slowness and connectivity issues, as can interference. Electronic items such as mobile phones and microwaves are among devices working on the same channels that can cause interference.

The choice of frequency comes down to intrinsic use of the network. 5ghz offers the best speed by utilising 802.11AC; 2.4ghz has a better range. In a whole school environment and even individual classrooms it would appear 2.4ghz – despite its limitations – might be a better option, even if 5ghz would appear to have the upper hand in some situations.

iv) Faster access points

In simple terms, a wireless access point (WAP) is a piece of hardware that connects wireless devices to the network via a router and precludes the need for messy and inconvenient wiring throughout schools. There are limitations as to how many devices can connect through one WAP without affecting performance so carefully pre-planning access point positioning is crucial.

Decide how many WAPs you will need and where to place them. They need to support all users and be able to accommodate future scalability. WAPs should be placed where there are the most users, such as in the classrooms, halls, examination rooms, common rooms and the staff room. Consider getting a wireless site survey or use heat map software to plan out where to position devices to provide the optimum coverage – a few vendors do provide this service free of charge (D-Link for instance).

It is important to check with the provider as to how many devices can be supported by each WAP and to ensure – even to the extent of actually physically going to look at every room or work space – whether there might be potential dead zones or areas where extra WAPs would be necessary. A successful network will cover the entire campus without interruption.

Hazle says: **"Always start at the end – know what outcome you desire and work out a way to get there. Think long term because you don't want a network rolling over because you add a few more devices. Each school is individual in its requirements but the aim in all is the same – to be able to use the equipment for teaching goals."**

Faster devices will become a necessity as the rate of pupil usage increases — not just downloading files and writing articles simultaneously, but maybe also looking at educational videos and messaging. Francis says: **"Our old system was slow and unreliable. For a new system we required over 500 devices with no loss of use. We now find the new system to be reliable with little down time. It is also easy to manage."**

v) Band steering

Band steering is a technology that detects whether or not the wireless client is dual-band capable, and if it is, it will push the client to connect to the less congested 5ghz network. It does this by actively blocking the client's attempts to associate with the 2.4ghz network. This enables latest technology use and backwards compatibility with existing legacy equipment.

The technology behind this innovation is the way 802.11 standard works, unless the SSID (wireless network identifier) is different between the 5ghz and the 2.4ghz networks, wireless clients will always connect to the 2.4ghz by default.

And because most Managed Wireless Networks tend to have a homogenous wireless network whereby the SSID is the same they may not be getting the most of their dual-band capable wireless network.

Since both 802.11n and the latest 802.11ac standards support 5ghz band, band steering can ensure that they achieve their maximum performance without being bottlenecked by legacy 802.11b/g clients.

Judd explains: **"The wireless radio is the device inside the wireless router that sends out the wireless signal. Most WAPs supply one radio, at best two. Each radio I guess has a client density ratio of 15:1 in a perfect world to maintain a healthy balance. We exceed that often.**

"Sixty-five per cent of our WAPs have two radios per base for 802.11n 2.4ghz and the other 35 per cent have two radios per base for 802.11n 2.4 and 5ghz and 802.11AC 5ghz access. In a perfect world I'd replace the 45 x 802.11n 2.4ghz units for the more powerful 5ghz AC units. We will look to buy five per year for the next five years to increase density and flexibility."

An important part of any local area network (LAN) is the network switch. This is an appliance that connects devices on a network and enables the transmission of data to specific targeted users rather than everyone, based on pre-programmed information.

In a multi-user network, therefore, switches play an integral role in managing the flow of data and increasing system efficiency and robustness. Standard switches are known as Layer 2 – with Layer 3 and core switches being the most advanced. Your ICT expert will advise how your LAN switches need to be configured. You need to ensure that switches are capable of dealing with or handling the traffic from the wireless infrastructure needed or being planned as part of the infrastructure may need to be upgraded to adequately deal with the traffic.

vi) Wireless AC Standard

The newest generation of Wi-Fi signalling in use is 802.11ac that utilises dual band wireless technology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz.

4. HOW SCHOOLS ARE UTILISING THEIR INFORMATION TECHNOLOGY INFRASTRUCTURE

i) 1:1 learning

This doesn't mean the ratio of staff to students, but the fact that every pupil has a PC/laptop/tablet/smartphone they can take home at the end of the day and continue to use for both educational and personal purposes.

Gone are the days when mobile devices were confiscated by staff at the school gate for fear of some sort of nefarious activity. Accepted wisdom now is that the use of personal devices in the classroom is a beneficial thing, if properly managed.

These benefits include:

Increased flexibility – schoolwork undertaken on the computer does not have to stop whenthe end of day school bell rings.

Students remain more focussed, engaged and comfortable when working on their own equipment.

Pupils are given more responsibility for their own learning - studies have reported an increase in the amount of work being done in a 1:1 environment. The discipline of learning is firmly on the shoulders of the student.

The equipment is often of a higher specification than the school could provide for every pupil.

Potential parent/guardian participation can be more easily encouraged when the mobile device is in the home each evening/weekend.

Teaching becomes learning - pupils are empowered to engage in deeper learning, analysis and creative thought as they become masters of the learning process.

Students can reach out to expertise outside the classroom and not wholly rely on the teacher as a source of information.

Collaboration/communication is increased as files are shared between pupils within school or at other schools.

Schools are less likely to be viewed as outmoded chalkboard establishments where going into the classroom is like stepping back in time.

Teachers spend less time dealing with IT issues and 'rote learning', leaving longer for quality teaching.

Teachers can adapt lessons with new technology and carry out activities not possible without mass internet access.

Social media sites deemed unnecessary and unwanted during the school day can easily be turned off through the network management system

ii) Managing BYOD

Bring your own device (BYOD) is the umbrella term describing the learning method by which pupils, students and teachers take in their own mobile device – often more powerful and capable than those provided by schools – and connect it to the school's wi-fi system, thus utilising the best possible tools available and enabling personal technology choice.

You might consider formulating a policy document clearly outlining the school's BYOD regulations to establish best practice and safeguard the integrity of both users and the network.

Managing this policy process should not be taken lightly. Network preparation is essential to ensure that your wi-fi network is robust, reliable and secure and scalable. Close scrutiny should also be given to resource implications, technical support, training, device specification, access to networks, teacher equipment, restrictions and limitations.

iii) Homework

Students, especially at a higher level, will be expected to undertake a great deal of work away from the school environment. Indeed, many schools now have portals allowing pupils to upload and download homework files, teaching documents, revision notes and past exam papers – as well as checking practical information such as timetable changes, activity bookings and field trips. The school has a duty of care to protect students from harmful material while they are on school property, but the responsibility falls back to the students and parents/guardians when the student is working at home – especially as they will be using their own equipment and continuing their studies from the classroom.

However, the issue of students accessing inappropriate material on their own device while out of school but on a school activity, such as a field trip or work placement, remains a grey area. Schools need a strong policy to cover this legally, possibly in conjunction with parents, as undoubtedly this challenging issue will raise its head at some stage.

5. MOBILE DEVICE MANAGEMENT (MDM)

i) What is MDM?

MDM is the accepted industry term describing the method of administering under one central umbrella a set of mobile devices such as tablets, laptops and smartphones using specifically-designed proprietary equipment. The beauty of MDM for schools is that a single IT specialist can maintain overall control for a wide variety of devices and it should be strongly considered as an integral part of any investment.

The ability to seamlessly and efficiently manage the various devices being used by pupils is an absolute necessity, for without a centralised management programme each device would need to be attended to individually for tracking, adding apps, passwords, security, software updates, announcements and so on . There would be scarcely time left for teaching.

Under-pressure educational establishments can use MDM to shift the emphasis for administering wireless networks away from the classroom back to the IT department where a small team of engineers can deal with an ever-increasing number of varied devices and manage them successfully within a wholly scalable enterprise. But they also enable technically-minded teachers to micro-manage classroom systems and access student devices to, say, transfer apps required by just one tutor group.

Schools' individual needs make it crucial that the right MDM system is utilised. There are many and varied types on the market, off the peg or bespoke, on-premises implementation or cloud-based and taking advice from experts is the obvious way ahead. The more flexible, dynamic and intuitive the system deployed, the more likely it is to be future-proofed and have an uncomplicated user interface.

It should be borne in mind that although MDM software is an integral tool for any wireless network solution, its efficacy is dependent in part on the nature of mobile devices on which it is being installed and it can be restricted by such limitations.

ii) Internet access

Safe and reliable connectivity is a key consideration for the introduction of any mobile learning platform.

The full management of access to the internet is a fundamental part of MDM. Web content browsing can be customised, filtered and/or restricted, depending on the school's requirements.

For instance, general internet access can be disabled for students, but not teachers, with all browsing routed through a dedicated channel. Access to key content and resources on the school's network can be controlled through a teacher/administrator console.

Judd says Parkstone Grammar's internet access is filtered and categorised through its software system with safety net technology behind its firewalls and Francis adds that all Wood End pupils log on using the school's secure web filtering.

Hazle says internet access regulations should be part of schools' policies, just like any potentially troublesome issues, with cyber bullying at the forefront - one of the biggest problems being the use of social media between pupils outside of school premises However, he believed that was a society issue as much as a school one.

"All students – and staff – need training to make them aware of what is acceptable and safe on the internet."

Schools may wish to adopt web filtering policies by which networks can be configured to give pupils secure connection to their network and prevent pupils connecting to open wireless networks. There may also be a need to prevent access to 'disruptive' features – such as messaging – during lesson times.

iii)Track data

The ability to track and review data is a prerequisite of any school network MDM system. You want to know who is doing what and when for educational, safety and security reasons within a framework of settings.

MDM systems have the capability to monitor actions undertaken by users, possibly by way of automated monitoring on specific topics. Once the mobile device is connected to the network it sends back information to a central point by a variety of means. How much data tracking is undertaken is down to personal preference.

iv) School firewall

With dozens, or possibly, hundreds of students all logged on to a school's network there is massive potential for the unwitting introduction of catastrophic malware, along with the threat of hackers attacking the core of your system.

With personal computers, laptops, tablets and smartphones at the heart of any network there is substantial and significant risk to both the network and individual users and so it is critical that adequate protection is enabled to keep devices safe and secure when online.

Students' own devices are naturally and inevitably storage centres for large amounts of personal information such as photographs, e-mail contacts, financial data and confidential documentation (even passwords), information that is attractive to criminals and malicious users.

Well-known threats include malware - which can introduce viruses, spyware, worms, and Trojan horses to devices – hacking, spam, pharming, phishing and botnets. In extreme circumstances these can lead to files being deleted or altered, sensitive information (such as passwords or credit card details) being copied or stolen, spam emails being sent out, security settings being disabled or loss of control of machines.

Thus all networks need the best possible protection through anti-virus software and firewalls. Anti-virus protection looks at files, downloads and emails, working as a barrier between network machines and the web, while a firewall offers defence against other devices attempting to access your network through the internet.

Computer operating systems sometimes have firewall protection built in, but wireless network administrators will want to find the best possible solution, such as a hardware firewall, from a credible company to give maximum protection for their users.

Hazle adds: **"A good firewall is essential, but will sometimes also block areas needed for schoolwork, however, calling for assistance to open up a browser can be seen as a small price to pay for the reassurance of protection."**

He says that malicious attacks on networks could come from inside or outside the system – with some savvy students possibly intent on trying to hack the system and of having the ability to do it.

One unwitting way that viruses could be introduced, Hazle says, is by way of plugging in USB sticks to transfer material. Not only is the student's work copied to the system but also, unknowingly, the hidden virus. Some schools have now banned their use.

v) Safety issues

The safety of pupils while using the internet at school is paramount and schools will have their own safety policies and may require pupils to sign an e-safety contract, its content dependent on age.

Pressnell says: **"Internet safety in schools and at home is obviously hugely important and it does bring challenges – especially with regard to supporting parents who may not be completely au fait with internet risks."**

These issues include cyber bullying, which knows no barriers and reaches across age, gender and social class.

There is also the potential exposure of pupils to offensive or upsetting material – such as pornography, graphic images, self-harming and radicalisation – is an unavoidable risk that comes with the advent of internet learning.

The onus is on schools to tackle cyber bullying and deal with it as effectively as they would handle the old fashioned playground bully. UK schools are all required by law to have measures in place to prevent bullying and cyber bullying.

Also, the risk of seeing offensive material can be significantly reduced through the use of leading-edge filtering and monitoring systems controlling which sites pupils can view and which are blocked.

Schools might need to update their general rules to take internet issues into account and act accordingly as technological changes and new issues come to light.

vi) Software updates

With pupils using their own devices there needs to be a method of updating them all – say with a new app or a system upgrade – other than by an IT manager doing each machine individually.

To attempt to do it individually on a system of more than just a handful of machines, say a class or a whole school, would prove completely impractical, time-consuming and disruptive.

The beauty of a Mobile Device Management system is that it enables software updates to be added to individual devices from a central point by a single operator as every machine is centrally connected.

It is advisable that schools should not consider rolling out 1:1 learning without an effective MDM system in place from the start.

6. ACCESS

Pupils – and staff - need to access the network easily without wasting valuable time navigating complicated entry procedures. A simple landing page where users enter their name and password is the fundamental basis of any network. The username and password can also be their existing login on authentication details. Pupil users would then see a customised desktop suited to their requirements; an easy to use interface being essential.

However, not all users need access to all areas of the network – for example, pupils don't need to see teaching resources and teachers don't necessarily need access to HR policies or accounts - and this can be regulated by an overarching ICT admission policy or the integration to segregation network using virtual LANs.

Schools generally have 4/5 virtual local area networks (VLANs) under one network (depending on the size of the school). A VLAN is a group of devices that may appear geographically separate, but are grouped together as if they existed in a LAN and thus enjoy the same management benefits and security and improve network performance.

The amount of network space available to users can thus be controlled in such a way that essential use is prioritised. Common policy is for teachers to have the biggest space, followed by office staff, pupils/students, guest users and outsiders/weekend users using techniques such as bandwidth management and Quality of Service.

Pressnell adds:

"Arnewood pupils log in with one user name and password regardless of where they are logging in on whichever device. Our system is simple and streamlined, but with a lot of technology behind it – elegant on the surface, but working furiously underneath."

7. TICKETING/BILLING

i) Ticketing

Primarily, this means a user being issued by the school reception with a 'ticket' (access code) to access a wi-fi system. Different, or higher, levels of access can be permitted depending on the user's needs. For instance, a local authority official may require complete access, a sixth former might be permitted social media access while a lower school pupil would have more restricted access.

The guest user is allowed temporary access to the system after entering a user name and a password assigned to them which is controlled by time or usage. System access is for a set time and once permission expires the guest would need to buy another ticket to carry on browsing alternatively the administrator can extend the usage time upon request.

Judd says that at Parkstone guest access is upon request and access/passwords are supplied after a booking to use the premises is made. Access is filtered using standard policies for pornography, gambling and so on. And Francis adds that all Wood End guests using the school's internet have to read and agree terms and conditions before they can log on.

With regard to in-hours visitors to schools, these will be overwhelmingly on the premises on school business in the form of local authority staff, trust representatives, supply teachers, outside consultants, parents and pupils from other schools. Therefore it may be prudent to at least offer a free wi-fi system during the school day.

One benefit of providing short term 'tickets' is that it allows schools to manage which areas can be accessed on the wireless network from a controlled environment. For example, a verified guest obtaining a ticket from reception would be allowed access to, say, social media sites or similar, which have been banned for students.

ii) Billing

Generally this is defined as buying internet access, usually with a credit/debit card through a secure automated process, on commercial premises where wi-fi hotspots have been established or by an online payment system such as PayPal.

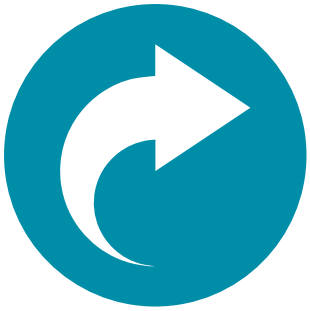
In the case of schools and colleges this would be mostly applicable during down times, such as evenings, weekends and school holidays when visitors such as community groups, adult education classes or conferences might be using school premises for their own activities and might require internet access.

This may well be considered 'free money' for schools since the wireless network is already in situ and no additional expense is required to monetise it – once a guest network has been established. This is done by configuring a ticketing/login system on the network and setting up a firewall permitting guests to access the login page only before payment is made and access permitted.

Having wi-fi available for guests may be deemed an inducement to attract more out- of-hours users to guest premises and also make money. However, the growing trend today is more towards offering free wi-fi at places used by the public – such as hotels, coffee shops, libraries, sports centres, airports, hospitals and shopping centres, so it is worth evaluating both methods before deciding which path to take.

Hazle says if schools find themselves able to charge for guest internet access they should take advantage, but this was more likely to be in rural areas where broadband generally might be otherwise slower or more sporadic than in city areas.

It is possible to run ticketing and billing systems side by side. This enables schools to facilitate free network use by authorised guest users through ticketing while at the same time charging outsiders to log on by way of billing.



8. FUTUREPROOFING

Creating a solid wireless network able to accommodate the exponential growth in devices and the use of outside applications is vital. Going beyond that network and seeing what other innovations are out there is, increasingly, also of paramount importance.

With devices becoming faster comes the need for the network to be able to cope. Thus future-proofing a system may require anticipating what changes might happen, because in our ever-advancing technological world the future happens quicker than ever.

For instance, where schools are developing new classrooms, blocks or even campuses there is a need to ensure the wi-fi network covers this. And there may well be a need for wi-fi access outdoors, such as on the sports field.

A new system, at the very least, needs future-proofing to the extent that it can be adapted to accommodate major change without user-disruption.

Judd says: **"Nothing can be absolutely future-proofed. We continue to invest in proven technology at a time that is economically viable and in line with best practice.**

"In a perfect world I'd rip out the legacy cabling and have it all re-done to current standards. I'd also embed a policy to refresh hardware every 18 months instead of when it 'no longer turns on', but that's not realistic.

"We have just VLAN'd the entire network to the edge switches, so we are in a better place this year than last. Next is to increase internet bandwidth on the curriculum from our fibre at 20mb to 50mb this year on contract."

Today's advanced technology means that network upgrades can be carried out gradually and in a piecemeal fashion without the need for disruptive system shutdowns. Incremental changes are also more budget-friendly and easier to manage than wholesale improvements

In general schools might well benefit from staying ahead of the game, by firstly investing in a robust, scalable wireless network then ensuring – through regular input from systems professionals – that the system is consistently checked and upgraded where necessary.

9. POLICY

The use of pupil-owned devices is growing exponentially and may well lead to school-supplied computers becoming less important, possibly in a similar way that the advance of interactive classroom whiteboards rendered blackboards obsolete.

It is something all schools will need to address and therefore it is essential to establish a strong policy, setting out the vision and the whys, wherefores, rules and regulations regarding wi-fi use. It is not something that can be taken lightly, nor approached in a half-hearted manner. Many schools have been embracing BYOD for years and have a policy in place, but they too need to constantly consider its contents and adapt to changing circumstances by renewing it regularly.

To formulate a policy will need a strategic approach, extensive planning and consultation, taking into account infrastructure, investment, training and resource implications. The implementation of a comprehensive and watertight policy will clearly state the school's position with regard to the use of mobile devices on school property. Nothing should be left to chance or open to misinterpretation.

But how to formulate a policy from scratch? Consult, consult, consult. Some schools will be able to take advice from their controlling local education authority (LEA) and, indeed, the LEA may make authority-wide policy decisions on their behalf. However, with many schools becoming academies and part of separately-funded educational trusts, it is more likely the trust will be in a position to offer guidance.

That said, perhaps the best approach is to consult with other schools already operating a technology use policy. Discussions with frontline users to get coalface opinions on the positive aspects and pitfalls could prove invaluable.

The buy-in of key stakeholders - staff and parents - is crucial. Teachers, in association with ICT departments, will be supervising a great deal more technology than previously and it is highly likely that parents will be funding the purchase of mobile devices.

10. PRACTICAL ISSUES

The smooth operation, sustainability and equitability of a wireless network system will lean heavily on the school's policy document, but there are day-to-day practical issues that need to be emphasised.

These may include:

- A detailed list of permitted devices
- Agreed hours of use
- Mandatory check-in procedure for students' devices
- The consequences of inappropriate use and clear responsibility parameters for the devices, their maintenance, management
- Security on site and when carrying devices to and from school.

There also needs to be a process for keeping the policy updated and communicated to stakeholders and a central register holding students' signed agreement slips is a must-have to indicate to staff which student has permission to bring what device to school.

Pressnell says: **"Any IT set-up has financial overheads. It is well worth the investment but is a recurring cost as technology does change. My advice is to buy a solution that is scalable – start small and grow.**

"The most important thing is staff training. Don't underestimate how long this will take. Staff have to be comfortable with using the system and buy into the vision. Any time spent in training will pay dividends time and time again."

In short, it is advisable for schools to remain flexible – decide what represents success, anticipate challenges, expect teething problems and respond to changes.

11. SUMMARY

There is no doubt that the use of mobile technology in schools will continue to grow exponentially, just as it has in life in general, and its complete incorporation within the educational system is seemingly inevitable.

Tablets, laptops, smartphones and other mobile devices have become the essential learning tools of today's classroom, giving easy and fast fingertip access to a world of knowledge unavailable to previous generations of pupils.

It is important, therefore, that schools give due consideration to working towards this modern way of learning and take into account a series of key factors that may well help smooth the path forwards.

The demand for instant information has radically changed the school environment forever and approaching this brave new world demands an embracement of the best technological practices available.

And today, that means utilising a robust and reliable wi-fi network capable of running hundreds of mobile devices that students bring in to school or to enhance and improve their learning experience and capability.

Expert guidance is needed so you don't buy too cheaply and a budget wi-fi solution leaves you with poor internet speed and patchy network coverage – or you buy a system too grand for your needs and you end up not needing much of its capability.

Therefore, informed decisions on choosing the most suitable technology cannot be made without support. The people in schools making these decisions, be they teachers, principals, heads or governors, need educating themselves on what they should be buying.

Checklist: How to get started

- [ ] Be certain what you want to achieve from your network and what represents success
- [ ] Understand how the whole process works
- [ ] Thoroughly research how other schools use technology
- [ ] Understand that technology intimately
- [ ] Don't take decisions in a hurry and without informed advice
- [ ] Call in industry professionals to guide you
- [ ] Ensure you have governor and senior staff support from the outset
- [ ] Agree a suitable budget and timescale
- [ ] Strive to get the initial infrastructure absolutely right through research, advice and professional help
- [ ] Look closely at futureproofing and scaling
- [ ] Set aside sufficient time for all staff to be trained
- [ ] Allow more than adequate time for staff to be trained away from the classroom environment
- [ ] Formulate a policy for mobile technology use
- [ ] Consider installing the best possible Mobile Device Management kit
- [ ] Control internet access, monitor data, combat bullying
- [ ] Remain vigilant against hacking, viruses with a strong firewall
- [ ] Regulate network access and wireless security mechanisms
- [ ] Consider ticketing and billing to grant different levels of internet access
- [ ] Always upgrade and improve your system
- [ ] Be flexible, anticipate pitfalls, expect delays
- [ ] Make sure you have a contingency budget

12. D-LINK

The network is the foundation upon which the delivery of enhanced teaching and learning via ICT depends. With the ever increasing importance of wireless technologies to support learning gains, it's imperative that your infrastructure can cope with the increasing demands being placed upon it – within perennially tight budgets.

D-Link's broad product portfolio consists of components for the core network as well as solutions to manage devices on the edge of the network including surveillance and storage components. For 30 years now, D-Link has been providing solutions that fit the requirements of education institutes.

13. SOURCES OF HELP

D-Link: http://www.dlink.com/uk/en

Levett Consultancy: https://levettconsultancy.co.uk/

NEN –The Education Network: http://www.nen.gov.uk/

Microsoft Bring Your Own Device in Schools: https://blogs.msdn.microsoft.com

Department of Education measures to keep children safe online: https://www.gov.uk/government/news/new-measures-to-keep-children-safe-online-at-school-and-at-home

Wood End Academy: http://www.woodendacademy.org.uk/

Parkstone Grammar School: http://www.parkstone.poole.sch.uk/

The Arnewood School: http://www.arnewood.hants.sch.uk/