The Education Network
Information Sheet 5
June 2014

Using consumer IT devices in schools

Smartphones, laptops, tablets, school-owned devices vs bring your own device (BYOD) and the consumerisation of IT

The Education Network
Information Sheet 5
June 2014
http://www.nen.gov.uk

Using consumer IT devices in schools

Options, opportunities and issues

Introduction

The phrase "the consumerisation of IT" describes the increasing affordability, availability, adoption and usage of personal, mobile internet-ready devices like laptops, tablets and smartphones. For a growing number of people, these devices offer an easier, more portable and accessible "always on" alternative for accessing the internet, sending and receiving messages and performing a wide range of other functions, from downloading apps and watching catch-up TV to making video calls and reading e-books.

Similarly, the increasing availability of broadband connectivity and Wi-Fi networks in homes, workplaces and public spaces provides new opportunities for using consumer IT devices for leisure, work and other activities, including potentially teaching and learning.

Another phrase often heard in this context is "bring your own device" (or BYOD), where people can use their own device to connect to a Wi-Fi network in their workplace or in public or shared spaces such as cafés, public libraries, universities, colleges or schools. While the BYOD model has and continues to receive much publicity, it is by no means the only model for using consumer IT devices in an educational context. For example, a number schools have purchased and are making very effective use of devices such as iPads in the classroom, with ownership of the devices remaining with the school.

This paper offers practical advice and guidance for schools wishing to find out more about the use of consumer IT devices in teaching and learning. It is divided into four sections:

1. The context and rationale for using consumer IT devices in schools
2. Management, planning and policy considerations
3. Using consumer IT devices in the classroom – opportunities and issues
4. Putting the right infrastructure and technology in place

This paper has been prepared by the NEN Technical Strategy Group and is intended primarily for school network managers, but is likely to be of interest to anyone considering how internet-ready consumer IT devices can be used in schools.

A note on terminology: throughout this paper, the general term "consumer IT device" is used to cover a broad range of devices such as laptops, tablets and smartphones. This term in itself does not imply where ownership resides (for example, with an individual pupil or member of staff), recognising that schools are already purchasing and using consumer IT devices in the classroom. The additional phrase "personally owned consumer IT device" (or similar wording) is used in this paper to denote where the use of devices not owned and/or managed by the school (i.e., devices that are brought into school premises by staff and/or pupils) is being considered.

Summary and recommendations

- The proliferation of consumer IT devices and broadband connectivity provides many new opportunities to support teaching and learning, both inside and outside schools.
- All schools need to be aware of these developments, regardless of whether the use of personal devices in school is to be supported or not; it is increasingly likely that over time more and more consumer IT devices will be brought into schools – by both pupils and staff.
- There are several models of consumer IT device usage, ranging from school purchased and provided/managed devices through to full bring your own device (BYOD) implementations.
- The complex issues and risks involved in supporting the effective and safe use of consumer IT devices necessitates a considered, strategic approach, particularly if devices are to be supported in large numbers.
- The safety of users and the security of school resources and data must be considered very carefully; updates and amendments to school IT acceptable use policies (AUPs), eSafeguarding policies, IT security and behaviour policies will be required. For example, how is staff access to school email from devices such as smartphones managed, ensuring that the school continues to meet its obligations in relation to the Data Protection Act and other requirements?
- It is likely that significant additional investment will be required to support the use of consumer IT devices by large numbers of pupils and staff, this and the management overheads of supporting the use of consumer IT devices may offset any immediate savings in device purchase and management costs.
- Communication with and agreement from staff, parents and pupils is crucial to the success of any initiative in this area, particularly in relation to what constitutes acceptable and unacceptable use and the sanctions that will be applied to deal with the latter. Many of the issues that arise from the use of consumer IT devices in schools are about culture and acceptance, rather than technology. All staff and parents need to buy into and completely agree the school's policy in this area if developments are to be successful.
- A comprehensive review of existing local and external networking and connectivity will be essential if the use of consumer IT devices is to be supported at scale.
- Local wireless networks need to be secure and offer performance and capacity to cope with significantly increased usage.
- Similarly, broadband internet connectivity needs to be able to support significantly increased volumes of traffic.
- Managed wireless and mobile device/enterprise mobility management (MDM/EMM) solutions may provide effective means to support large numbers of devices.
- Any implementations must be able to scale to accommodate increased usage as both device take-up and broadband usage are continuing to increase year on year.
- Schools should seek professional advice before embarking upon any large scale initiative in this area.

1. The context and rationale for using consumer IT devices in schools

The consumerisation of IT – where more and more people are using low-cost, highly portable, mobile wireless enabled devices like smartphones and tablets – is changing the way technology is used for work, leisure and a range of other activities, including teaching and learning.

In August 2013, Ofcom, the UK communications regulator, reported that over half of adults (51%) now own a smartphone, almost double the proportion two years ago (27%). At the same time, tablet ownership has more than doubled in the past year, rising from 11% of homes to 24%. The average household now owns more than three types of internet enabled device, with one in five owning six or more.[1]

In October 2013, Ofcom reported that among 8-11 year olds:

> "…18% now own a smartphone, and the same proportion own a tablet computer. While the smartphone figure is largely stable year-on-year, tablet ownership has grown four-fold among 8-11s since last year (from 4%)…younger and older children have different priorities when it comes to connected devices. Among older children (12-15), smartphones remain more widely used than tablets. Around three in five (62%) own a smartphone – unchanged since last year – but 26% now own a tablet computer, up from just 7% last year. The use of tablets has tripled among 5-15s since 2012 (42%, up from 14%), and one quarter (28%) of infants aged 3-4 now use a tablet computer at home."[2]

Take-up of faster connectivity is also increasing: Ofcom research into UK fixed-line broadband performance reveals that one in four UK residential fixed broadband connections is now superfast, i.e. offers a headline speed of 30Mbps or more.[3] The increasing availability of ever faster fixed and mobile broadband services and Wi-Fi networks creates ever more opportunities to connect to the internet. Users can be online all the time via their device (or devices, as many people now have more than one); many devices can connect via both Wi-Fi and mobile broadband (3G or 4G) networks. At home, users might connect to their Wi-Fi network, underpinned by a superfast broadband service. When they are out and about, they may primarily be online via 3G or 4G mobile broadband networks, but may also connect to public Wi-Fi services (hotspots) in cafés, public libraries and other locations where these are available.

Many users seek to use Wi-Fi networks wherever possible, to minimise the amount of data they download over 3G or 4G mobile networks: most mobile data tariffs are based on not exceeding a monthly download "cap" (for example, 250MB or 1GB), and are priced accordingly. One device might connect by sharing another device's connectivity; for example, a tablet or laptop might connect to the internet by tethering to a smartphone via Bluetooth.

[1] http://media.ofcom.org.uk/2013/08/01/the-reinvention-of-the-1950s-living-room-2/
[2] http://media.ofcom.org.uk/2013/10/03/younger-children-turn-from-phones-to-tablets/
[3] http://media.ofcom.org.uk/2014/04/15/uk-experiences-superfast-broadband-surge-but-challenges-remain-to-address-speed-mismatches/

People now expect to be online all the time wherever they are as a matter of course. Many employees now carry their own powerful IT devices with them all the time and are keen to use them in the workplace. At the same time, employers recognise the potential to increase productivity and improve job satisfaction if employees are allowed to and supported in doing so.

As a result, many employers are starting to embrace the use of personally owned devices, ensuring that user agreements and technical measures to ensure appropriate usage are in place and understood. This trend is often referred to as "bring your own device", or BYOD (sometimes "bring your own technology", or BYOT). According to Cisco, BYOD is a "megatrend": "IT managers are establishing policies with BYOD access as the norm rather than the exception due to increasing demands from employees and executives who embrace this megatrend."[4]

Consumer IT devices can offer a range of similar opportunities for schools. For example, they can support the personalisation of learning, where learners use a device they are already familiar and comfortable with. They also offer the potential for increased learner and parental engagement if devices are used both at home and in school, providing continuity of learning and bridging formal and informal learning.

Practical advantages of consumer IT devices include their affordability, ease of use, instant on from standby (as opposed to a lengthy boot up time), multiple connectivity options and long battery life. Downsides include unpredictability of cost (particularly in relation to mobile broadband services) and variations in functionality as a consequence of different operating systems, software and screen sizes.

Educational uses include note taking, collaborating on class assignments, internet research and accessing cloud based education applications. The increased availability of cloud services and applications is another factor driving take-up of both consumer IT devices and mobile broadband services: applications and data hosted in the internet "cloud" can be accessed from anywhere from any connected device.

The IT industry is responding accordingly, both in terms of the increasing number and range of consumer IT devices now available and the infrastructure and tools needed to support an effective BYOD implementation. However, it is important to recognise that there are several potential models for using consumer IT devices in schools, including but not limited to BYOD. For example, a school may wish to purchase and retain ownership of a set of consumer IT devices, which may also be loaned for use outside the school, but may not wish to support the use of personally owned devices being brought into school. Similarly, a school may wish to support the use of certain types of consumer IT device but not others, or may wish to support the use of personally owned consumer IT devices by staff rather than pupils.

[4] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Solution_Overview.html

This paper sets out the range of options, opportunities and issues schools should be aware of in relation to the use of consumer IT devices to support their planning and decision making in this area. While consumer IT devices offer many opportunities for schools, there are many challenges and potential pitfalls too, necessitating a considered, strategic approach.

The expectations of learners, parents and staff need to be understood and managed appropriately, especially if/when devices are brought into schools on a regular basis by staff or pupils or both. It is recommended that all schools should develop a position on the use of consumer IT devices, which should be kept under regular review.

It is hoped that this paper will assist schools in doing so. The rest of this paper is structured as follows:

- **Part 2** describes the management and policy issues schools should consider at a strategic level;
- **Part 3** considers the ways consumer IT devices can be used in the classroom;
- **Part 4** outlines the infrastructure and technology that need to be in place if consumer IT devices are to be used successfully in schools.

Implementing the use of consumer IT devices is by no means mandatory for schools. However, the increased take-up of consumer IT devices and increasing expectations for both the availability and speed of broadband connectivity are clearly now irreversible trends. All schools now need to consider their position in this area; with the right policy and technology frameworks in place, consumer IT devices can be very effective in supporting teaching and learning in schools.

A note on terminology: throughout this paper, the general term "consumer IT device" is used to cover a broad range of devices such as laptops, tablets and smartphones. This term in itself does not imply where ownership resides (for example, with an individual pupil or member of staff), in recognition that schools are already purchasing and using consumer IT devices in the classroom. The additional phrase "personally owned consumer IT device" (or similar wording) is used in this paper to denote where the use of devices **not** owned and/or managed by the school (i.e., devices that are brought into school premises by staff and/or pupils) is being considered.

2. Management, planning and policy considerations

The complexities of using consumer IT devices in schools necessitates a considered, strategic approach if the many potential pitfalls are to be avoided. This section provides an overview of the key policy aspects schools' senior leadership teams should consider before embarking on any implementation.

Objectives and fit with overall institutional policy and strategy

The first and most important activity is to determine the objectives for supporting the use of consumer IT devices. These should be in keeping with the school's overall strategy and policy for teaching and learning: the use of consumer IT devices should be driven by clearly defined teaching and learning goals, rather than technology goals. Consideration should also be given to how progress towards these goals will be measured and how any additional benefits will be evaluated. Implementing a new policy as complex as using consumer IT devices in schools simply because it is possible to do so, or because others are seen to be doing so, are not sufficient reasons in themselves.

As with any new initiative, early and regular consultation and communication with all stakeholders is essential. Stakeholders include school staff, governors, parents, pupils and ICT support services and suppliers. Implementing the use of consumer IT devices will generally be a significant organisational change, requiring additional training for teaching and support staff. Similarly, the complexity of using consumer IT devices means that any implementation should be planned carefully and introduced in incremental steps and phases. For example, you may wish to trial a small number of devices of a particular type first, to explore their potential, or you may invite a couple of members of staff to explore the use of their own devices in school and report back. The evaluation of such pilot schemes is a very important phase of the assessment and implementation process and is often overlooked. A "big bang" implementation approach is very unlikely to be successful.

Budget and cost issues

It is very tempting to regard any move towards the use of consumer IT devices (especially where devices are not purchased and managed by the school) as an opportunity to save money as a result of no longer having to buy and maintain expensive IT facilities such as desktop and laptop computers and software licences. However, this is a very short-sighted view.

As stated previously, there are a number approaches to using consumer IT devices in schools, with some based on the school retaining ownership of devices. Clearly, in these models, such device savings will not apply. But even in models that are based on personally owned devices being used in school, the infrastructure upgrades and organisational changes that will be required will incur significant costs. These might include upgrading school Wi-Fi and broadband connectivity to accommodate the increased number of devices using them, or potentially the cost of implementing full mobile device management (MDM) and managed Wi-Fi solutions. These options are discussed in more detail in part 4 of this paper.

Additionally, given the limitations of consumer IT devices for complex operations, it is highly unlikely that any school would currently wish to migrate fully from school-owned and maintained desktops and laptops: many school IT applications and activities are dependent upon the greater computing power, standardisation and flexibility of desktops and laptops. The use of consumer IT devices in most cases is likely to augment the continued use of such "traditional" devices in schools, just as tablets and smartphones complement the continued use of desktops and laptops in business environments.

The bottom line is that cost saving should not be a driver for implementing the use of consumer IT devices in schools. Any immediate savings in device purchase and management costs may well be offset if not exceeded by additional expenditure elsewhere. Schools need to consider the total cost of ownership (TCO) of any model of consumer IT device usage, bearing in mind that some costs are more visible than others. For example, the amount of training and school network re-engineering that different solutions involve both need to be considered, as these will have both significant financial and resource (time) implications for schools. In addition, schools should also factor in the costs of carrying out a full risk assessment prior to deployment for the data, services and information systems that may/will be accessible as part of any proposed implementation. The risks of information and data leakage could be significant and schools should not underestimate the potential consequences from a data protection or indeed a safeguarding perspective.

Personal device ownership, deployment and usage models

As discussed previously, there are a number of different options for implementing the use of consumer IT devices in schools. Each has its own strengths, weaknesses, opportunities and issues; which (if any) model is best suited to a particular school is a matter for individual determination. No one model is right or wrong, or best or worst; schools need to make an informed decision as to the model or models best suited to their circumstances and aspirations, recognising that these will change over time.

Models can be differentiated in terms of:

- **Devices –** what devices may and may not be used in the school, and for what purposes?
- **Ownership** – who owns the device, and who is responsible for managing and maintaining it?
- **Functionality** – can devices be connected to the school's network, or can they be used only as stand-alone devices? If they are allowed to connect to the school's network, what can they do once they've done so (access the Internet, access local network services)? How will devices interoperate with the school's existing devices and systems?
- **Management and control** – how much control is there over which devices can be used in school, and (if allowed) how they connect to the school's network? How are these aspects enforced?

- **Monitoring and accountability** – lessons which have been learnt over the last 10 or so years should not be forgotten in relation to the eSafeguarding elements of any proposed deployment. How will device usage be managed, tracked and monitored? How will monitoring information be reviewed and acted upon in order to prevent a potential data security or safeguarding incident, or retrospectively should such an incident occur?
- **Risk** – using consumer IT devices in schools brings risks as well as opportunities (for example, there is a risk that viruses and malware could infect the school's network from a personal device, or that personal data might be lost); what are the risks (to the school, to the pupil, to the member of staff) in each instance and how can they be mitigated?

In broad terms, potential consumer IT device ownership, deployment and usage models include the following:

- School purchased / owned / maintained devices that are used only in school
- School purchased / owned / maintained devices that are used in school and can also be loaned to pupils for use at home and elsewhere
- School specified but parent purchased single device – "standard issue"; device is maintained by / remains responsibility of parent / learner (offers procurement aggregation opportunity if school coordinates purchase?)
- School specified range of devices (laptops, tablets etc.) – parent purchased, device(s) is / are maintained by / responsibility of parent / learner (offers procurement aggregation opportunity if school coordinates purchase?)
- Minimum specification set by school (screen size, operating system, processor speed, software required) – affords wide choice of device, but places significant responsibility on parent / learner to ensure any device purchased meets the minimum specification (enforcement?)
- Any connect-able, internet-ready device can be brought in / used in school – full bring your own device, "anything goes"

This list of options forms a continuum: those towards the top provide schools with the most standardization, involve the greatest device management overhead and offer the lowest risk and least flexibility. Conversely, the ones toward the bottom provide schools with less or no standardization, involve the lowest or no device management overhead and offer the highest risk and greatest flexibility. Similarly, models towards the top are likely to require less modification and upgrade of schools' existing Wi-Fi and broadband infrastructure, while those towards the bottom are likely to require the most, especially if it is anticipated that a large number of consumer IT devices will be brought into and used on school premises.

These models are not mutually exclusive and can potentially co-exist, though this in itself will create a significant additional overhead. A school might wish to deploy one of the models above for certain types of device (or for a particular group of pupils or staff) and a different model for others.

For example, a school may wish to adopt a hybrid approach, defining a minimum specification for parent purchased pupil laptops that will be used in school to access both the internet and local network services and resources. At the same time, it may allow that any capable device may be brought into school and used to access the internet via the school's Wi-Fi network, but cannot be used to access internal school network services and resources directly. Similarly, some types of device may be allowed to be brought in and used in school, but may not be connected to the school's wireless network.

Schools' senior management teams thus need to consider their user, device and functionality requirements at as granular a level as possible, in close consultation with pupils, parents and staff. This will enable the identification of the most appropriate model(s) and will ensure that the school can frame its policy or policies in this area in keeping with its overall organisational objectives and available resources.

Equity and ownership issues and considerations

While devices are becoming ever more affordable and take-up continues to increase, it should not be taken for granted that every child will be equipped with a device by their parents or guardians. If access to a consumer IT device is deemed essential, schools will need to consider how they will ensure every child has access to a device to avoid a "digital divide". Options include purchasing a set of loan devices for children to use in school and potentially elsewhere as well.

Another approach is to set up an assisted purchasing scheme; the e-Learning Foundation[5] provide support and guidance in this area. All approaches require sensitive management to ensure children using loan devices or devices sourced through assisted purchase schemes are not stigmatised as a result. Equity issues do not relate solely to device costs; not every home has access to broadband connectivity, either because of cost or geographical issues; software licensing and app purchase costs could also be a cause of inequality and concern.

Careful thought also needs to be given to the use of personally owned devices in schools, to limit schools' liabilities in relation to issues such as insurance, technical support, breakages, information contamination (defining the demarcation between personal and school owned information) and theft. Clear communications with parents are essential to ensure pupils, parents and staff are aware of and understand all their responsibilities, which should be clearly set out in the appropriate school policy documentation. The use of personally owned devices in a school is likely to require a policy in its own right, as well as amendments to schools' existing policies, such as eSafeguarding, behaviour and IT acceptable use documents. As with all school policy documents, a policy for the use of personally owned devices should be kept under regular review.

[5] http://www.e-learningfoundation.com

Acceptable use and e-safety – policy (not technical) aspects

As with any technology, supporting consumer IT devices in schools offers the potential for misuse as well as opportunities to support teaching, learning and administrative functions. Schools should draw up guidelines as to what constitutes appropriate and inappropriate use; the potential for consumer IT devices to disrupt the classroom if not appropriately managed has led some commentators to re-christen BYOD as "bring your own distraction". Devices with in-built 3G or 4G mobile connectivity offer a particular set of challenges: if mobile network coverage is available in the school, such devices can connect directly to the internet, bypassing the school's network entirely.

Usage guidelines should be incorporated into schools' existing policies (for example, school behaviour, eSafeguarding, code of conduct and IT acceptable use policies); as mentioned previously it is likely that the use of personally owned consumer IT devices in schools warrants a policy in its own right, covering acceptable and unacceptable usage, the sanctions for inappropriate use and the responsibilities and liabilities of pupils, parents and staff. This policy could take the form of a parent/pupil user agreement which is signed by both pupils and parents; an example is included in Appendix 1 of this document.

There are a number of technical approaches that can be employed to help ensure that consumer IT devices are used safely in schools without compromising school or individual data security. These are discussed further in section 4 of this document.

3. Using consumer IT devices in the classroom – opportunities and issues

Some aspects and questions to consider in relation to the use of consumer IT devices in the classroom include:

Classroom management/device usage:

- How to maximise the opportunities presented by consumer IT devices?
- How to integrate technology enabled learning into the curriculum?
- Consumer IT devices are likely to augment, not replace, established teaching and learning methods; they are also likely to be complementary to "traditional" IT equipment (laptops, desktops), which will remain the best tools for certain applications and activities
- Consider the possibilities of the "flipped classroom[6]" – "any use of technology to leverage the learning in a classroom, so a teacher can spend more time interacting with students instead of lecturing"
- What will staff and learners use their connected devices for – why choose consumer IT devices?
- Strategies for ensuring appropriate/responsible usage must be in place
- Some devices are designed primarily for content consumption (for example, watching videos) rather than content creation (such as complex documents or spreadsheets)
- The potential for device diversification needs to be considered carefully – should expectations be based on the least powerful/functional device in the classroom, or the most advanced/capable device?
- End-user support expectations must also be set and managed appropriately– teachers should not be expected to know the ins and outs of every device, nor be responsible for them if they are not owned and provided by the school
- Clear demarcation is necessary between teacher, school network support & learner/parental responsibilities and obligations

Device considerations:

- Different consumer IT devices offer different benefits, functionality and challenges: smartphones, tablets, netbooks and laptops all have very different capabilities, advantages and disadvantages
- Functionality and capability considerations in any mixed device environment are important – should the approach in the classroom cater for the capabilities of the most basic device, or the most advanced?
- Managing/ensuring consistent apps and content on multiple devices – how will this be achieved?
- To what extent will the content and services you currently use in the classroom work across the range of personal devices and operating systems? (iOS, Android, smartphones, tablets, netbooks, laptops)
- Charging and device battery life – how will this be managed to ensure as much "uptime" as possible and minimise disruption? Should any BYOD home/school agreement require that devices are brought to school fully charged?

[6] http://en.wikipedia.org/wiki/Flip_teaching

4. Putting the right infrastructure and technology in place

Supporting the use of consumer IT devices in schools can place a significant additional load on school networks, ICT support and broadband connectivity. A review and audit of existing infrastructure and capability is essential, to determine whether the use of consumer IT devices at the scale anticipated can be supported via existing facilities or whether upgrades will be required. The extent of any required upgrade will be dependent upon the device deployment model or models to be adopted (see section 2).

The two most important infrastructure components to consider are internal wireless networks (including coverage, performance, capability and security) and external broadband and internet connectivity, especially if it is envisaged that a large number of consumer IT devices will be supported. Both initial and likely future requirements need to be taken into account.

The following seven questions provide a basis for identifying and quantifying infrastructure requirements, and the consequential extent of any technology refresh or upgrade:

1. What model or models of consumer IT device usage do you want to follow? Different models have different implications for school IT infrastructure and support (see section 2).
2. How many devices/concurrent users do you envisage will there be, both now and in the future? Bear in mind that in some contexts, users may have more than one device they want to connect to the school's network at any one time.
3. Which type or types of devices do you want to support – tablets, smartphones, laptops? Different types of device and operating system (iOS, Android, BlackBerry, Windows) have very different management and support issues, overheads and requirements.
4. What do you want users to be able to do with/access from their devices? What are the bandwidth requirements of the applications and services you expect them to use? Internet/public cloud only? Internal network services & resources? Printers?
5. Where and when do you want users to be able to use their devices – throughout the school or only in specific areas? Throughout the school day or only at certain times?
6. How will you ensure that the security of your internal networks and systems are not compromised, and that users and their data are kept safe and secure?
7. How will you manage authentication of users from personally owned devices and how will device usage be tracked and monitored? Who will act on this information and how/when?

Wireless network coverage, performance and capacity

An effective wireless network is a prerequisite if consumer IT devices are to be used successfully in a school environment. Most devices now offer Wi-Fi (wireless LAN) connectivity, for use wherever a suitable Wi-Fi network is available: such locations include private networks in homes and businesses,

and public networks in cafés, hotels, libraries and an ever increasing range of other public and shared spaces.

Ofcom reports than Wi-Fi is now the primary mechanism for smartphones to access data and that usage continues to increase:

> "Most smartphones now have Wi-Fi capability, and the majority of the data consumed on mobile devices is currently carried using this Wi-Fi capability, rather than over cellular networks…The number of public Wi-Fi hotspots has more than doubled and the average data consumed at each hotspot has also increased. The combined effect is that public Wi-Fi traffic has grown by over 190% over the last year…Despite this, public Wi-Fi off-load is still small when compared with off-load onto private Wi-Fi. We expect operators and equipment vendors to make discovering and connecting to public Wi-Fi networks more seamless over the coming year, using technology standards such as Passpoint, and this should result in significant further growth."[7]

The increasing reliance on Wi-Fi for connectivity and the requirement to support devices across a range of locations now mean that enterprise grade, professionally deployed wireless networks are required if large scale usage of consumer IT devices is to be supported. In future, users will increasingly expect to be able to connect more than one device at a time (for example, both a smartphone and a tablet), further increasing the loads on wireless networks. Additional drivers specific to the education sector are the facts that online learning applications are often based on multimedia content (particularly video) and that they require a high degree of interactivity, both of which can place significant additional loads on wireless networks and broadband connectivity.

Deploying and managing a large scale, high performance Wi-Fi network across a school is not a trivial task. Wi-Fi networks need to be carefully planned if they are to support the effective use of a large number of devices, applications and content across a range of locations. Standards-based technologies and solutions are available to assist schools in this regard. The IEEE 802.11n and the emerging 802.11ac wireless networking standards provide much faster data rates than previous standards (802.11a, 802.11g), designed to meet the demands of more users, more devices and more data. In addition, companies such as Aerohive, Aruba, Cisco Meraki, Meru, Motorola and Ruckus (see Appendix 2) now provide complete provisioning, management and security solutions for wireless networks, simplifying and centralising the day to day management of complex, large scale wireless networks. These solutions are designed to support large numbers of devices, users and applications whilst keeping users and data safe and secure.

Schools now require the same attributes and features (throughput, scalability, reliability, security, ease of provisioning and management, affordability) from their wireless networks as businesses, particularly in relation to supporting large numbers of devices, and the marketplace is responding accordingly. Any school considering a large scale implementation or upgrade of its wireless network should review its requirements carefully and seek professional advice before proceeding.

[7] http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/infrastructure-report-2013/

Diversity of devices and operating systems – mobile device management (MDM) solutions

Depending on the deployment model or models adopted (see section 2), schools may wish to support a wide variety of devices (tablets, smartphones, laptops) and operating systems (such as Apple's iOS and OSX, Android, BlackBerry and Windows). The different capabilities and limitations of devices can make this a complex task, with certain devices requiring a particular configuration in order to connect to an enterprise or educational network.

Additionally, access needs to be provided in a way that does not compromise network or data security, or allow inappropriate content to be brought into school. Devices need to be monitored and prevented from causing damage to school networks and services. For example, "jailbreaking" Apple iOS devices allows devices originally locked for use with a particular mobile network to be used on other operators' networks, as well as allowing additional apps, extensions and themes unavailable through the official Apple App Store to be downloaded and run. Similarly, "rooting" an Android device can overcome the limitations that carriers and hardware manufacturers place on some devices, resulting in the ability to alter or replace system applications and settings, run specialized apps that require administrator-level permissions, or perform other operations that are otherwise inaccessible to a normal Android user.

Jailbroken and rooted devices clearly offer a higher level of potential risk than standard devices, but effective mechanisms need to be in place to manage the risks inherent to all devices that are allowed to connect to the school's network. Devices that have their own connectivity to the internet (either on the device itself or by connecting via a different device) can represent a serious security threat as they offer a "back door" access for infectious malware. Once connected to a network (e.g. a WAN) they then have access to centralised devices, posing a real threat that is probably far greater than that posed by more traditional means of bringing in malware via removable media such as USB sticks, CDs or DVDs.

This diversity of devices, operating systems and related risks can create a significant technical support overhead if not managed appropriately, as users struggle to connect their device to a school's network, or find that their device or applications do not work as expected once they are connected. Similarly, schools need to be confident that the consumer IT devices they provide access to can be managed so that they cannot compromise the security of their networks and the safety of their users. Devices, operating systems and applications are all updated frequently, creating a series of moving targets for network support staff.

By way of an example, Yorkshire and Humberside Grid for Learning (YHGfL) has published a technical white paper setting out the issues involved in deploying Apple iOS devices in schools, identifying how these devices and applications do not use traditional internet protocols.[8] Other operating systems and devices may pose similar issues for schools, particularly where devices have been developed primarily for use in residential rather than enterprise environments.

[8] http://www.yhgfl.net/Support/White-papers/Advice-and-guidance

Mobile device management (MDM) solutions have emerged in response to the increasing use of consumer IT devices in business and educational environments, to address the configuration management challenges and issues they present. MDM solutions offer a means to maintain central visibility and control over a wide variety of devices, determining how they connect to corporate networks and what they are able to do once they have done so, providing or restricting access to services and data as required. They can also manage the delivery of any required content and applications to devices, as well as providing security features such as the capability to wipe applications and data from any devices reported lost or stolen.

This is a rapidly developing area, with MDM solutions offering an increasing range of functionality (including device, application, content, security and identity management), as mobile devices, operating systems and applications continue to mature and diversify. Enterprise mobility management (EMM) is another term used in this context to describe the broader set of functionality solutions are beginning to offer, encompassing MDM alongside additional related capabilities. Companies providing solutions include Airwatch, Cisco Meraki, Lightspeed and Maas360 (see Appendix 2). MDM/EMM solutions can assist with the management and administration of school owned and provided devices, as well as provide a means to control personally owned devices as part of a BYOD initiative.

Schools need to understand the capabilities and limitations of all the classes of device and operating system they intend to support, recognising the inherent differences between them. MDM/EMM solutions may offer a cost-effective means to support the effective use of consumer IT devices, particularly where large numbers of diverse devices are to be supported. As with wireless networks, schools should seek professional advice before embarking on any procurement or implementation in this area.

Security – of networks, users, devices and data

Schools need to be able to secure and manage how consumer IT devices access their networks, to distribute, support, monitor and control the use of applications and content and to protect and secure school networks, data and users.

The reach of a school's wireless network may extend beyond its buildings and grounds, particularly in densely populated urban areas, so a mechanism to prevent unauthorised access from outside the school is likely to be required. This echoes the situation in residential and business premises, where a number of wireless networks can generally be picked up from within a single premise, including the premise's own network as well as those of several neighbours.

A fundamental requirement is authentication, to ensure that only those entitled to access the school's network are identified and authorised to do so. Issues to consider include:

- How will you distinguish different classes of users (pupils, year groups, teaching staff, administrative staff) and devices, tailoring policies and access accordingly?

- Do you need to restrict the use of certain devices during certain hours of the day for certain groups of users?
- How often will teachers, staff and students need to re-authenticate?
- What authentication mechanisms are currently in place for existing networks and resources? Can these be adapted to support access from a broader range of devices, including personally owned devices?
- Do you need to provide temporary access for guests? How will authentication be managed if so?

Network security can be maintained by ensuring appropriate separation and segmentation of networks and resources. Virtual local area networks (VLANs) and additional service set identifiers (SSIDs – the wireless network name that appears on devices when they scan for available networks) for wireless networks can be implemented to separate devices and users appropriately. Again, the managed wireless network and mobile device management solutions discussed previously may be of considerable assistance here, especially for large scale deployments.

Such technical strategies and approaches can help to keep school networks, resources and data separate so that only authorised users are able to access them. It is very important to consider "worst case" scenarios when planning in this area. For example, what happens if a device is lost or stolen? Can access be barred from that device as a result? Can school data and applications be wiped from a lost or stolen device? Are any mechanisms or facilities in place to "sandbox" (a tightly controlled set of resources to isolate services and data[9]) school information and resources? It is essential to consider the risks as well as the benefits of providing access from consumer IT devices, to prevent loss of and inappropriate access to personal information. Amending or drawing up a school IT security policy is particularly important in this context, this may well need to be additional to and separate from a school's IT acceptable use policy (AUP).[11] The Information Commissioner's Office (ICO) has published advice on keeping personal data safe and secure as part of a bring your own device (BYOD) implementation; whilst primarily intended for businesses, many of the principles it describes are equally applicable to schools.[12] Archived advice on data security schools published previously by Becta may also be of assistance.[13]

It is also important to ensure personal devices are used appropriately to keep all users safe and secure; schools should set and communicate what is expected from all users in this regard, as well as the sanctions for inappropriate use, as discussed previously in section 2.

[9] http://en.wikipedia.org/wiki/Sandbox_(computer_security)

[11] For examples, see http://www.lgfl.net/esafety/Pages/data-security.aspx

[12] http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx

[13] http://webarchive.nationalarchives.gov.uk/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

External connectivity – broadband and internet access

Large numbers of consumer IT devices can place a significant additional load on school broadband and Internet connectivity as well as on local area network infrastructure.

From NEN Information Sheet 4, *Selecting broadband connectivity for your school*:[14]

> "The line speed and capacity of the school connection has to be modelled to meet the educational, management and communications usage which are dependent on the size of the school, the applications being used to deliver teaching and learning and to support the management and operation of the school.
>
> Schools' use varies depending on the educational strategy and management practices of the institution. The following lists some of the typical uses but is not exhaustive. When assessing broadband requirements, it is important to fully understand the applications currently supported or likely to be required to deliver the educational and management outcomes of the schools strategic development plans:
>
> - Pupil Internet Access for research – browsing including video and images.
> - Staff use for class teaching including real time applications (talking books, iPlayer, You Tube).
> - Staff mail with attachments.
> - Pupil email.
> - School Office functions including MIS.
> - School portal, website or VLE.
> - Pupil use of cloud based functions VLE, Google Apps, Office 365 etc.
> - Cross school or cross site working and support for ICT.
> - IP communications VoIP, Video, Skype
> - Closed Circuit TV.
> - Schools operational systems, remote access and reporting for functions such as energy consumption, catering systems etc.
> - Multi-Agency requirements."

Consumer IT devices now offer sufficient performance and capability to undertake most if not all of the functions described above, greatly increasing the volume traffic traversing both the school's local area network and broadband Internet connection if used in large numbers by both pupils and staff.

[14] http://www.nen.gov.uk/files/NEN_InfoSheet_4_Selecting_Broadband_Connectivity.pdf

Broadband speeds and usage are increasing across the board. Ofcom reports that the proportion of superfast connections rose from 5% in November 2011 to 25% in November 2013, while the average superfast connection speed has continued to rise, reaching 47.0Mbps by November 2013 – an increase of 47%, or 15.1Mbps since May 2010. At 17.8Mbps, the average actual fixed-line residential broadband speed in the UK is almost five times faster than it was five years ago when Ofcom first began publishing this data.[15] Previous Ofcom data[16] reports that:

- the average broadband speed has more than quadrupled since Ofcom first began publishing speeds data in November 2008 – an increase of 309% (or 11.1Mbps).
- Around 4.8m UK customers have taken up superfast broadband, up from 2.1m in 2012.
- The average data used on uncapped superfast broadband services in June 2013 was 55GB, whereas customers on uncapped ADSL2+ technologies used an average of 26GB.

The UK Broadband Stakeholder Group (BSG) estimates that the median household will require bandwidth of 19Mbps by 2023, whilst the top 1% of high usage households will have demand of 35-39Mbps.[18]

These figures provide a benchmark for what users increasingly expect to be able to do with their devices; schools need to plan carefully to ensure that their broadband and Internet connectivity can scale appropriately in the light of increased future demand, particularly if it is envisaged that large numbers of consumer IT devices will be connecting to the school's network simultaneously.

Again, from *Selecting broadband connectivity for your school*, based on providing 2Mbps per user:

"1. For a secondary school with 1600 pupils and 400 connected devices.

2Mbps per user download for a school with 400 devices = 800Mbps. Allowing for 1 in 10 devices being active simultaneously at times of peak demand means that the connection capacity should be 80Mbps.

The requirement for a 100Mbps connection for a secondary school has already been exceeded in that the best connected schools in the UK have 1Gbps connections.

2. For a primary school with 200 pupils and 40 connected devices

For a primary school with say 40 devices = 80Mb and assuming 1 in 10 devices are simultaneously active at times of peak usage = 8Mbps

Measurements taken in primary and special schools with good educational broadband use indicate that actual usage in 2012 shows peaks over 10Mbps.

[15] http://media.ofcom.org.uk/2014/04/15/uk-experiences-superfast-broadband-surge-but-challenges-remain-to-address-speed-mismatches/

[16] http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/broadband-speeds-may2013/ & http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/infrastructure-report-2013/

[18] http://www.broadbanduk.org/2013/11/05/bsg-publishes-new-model-for-analysing-domestic-demand-for-bandwidth/

This is a conservative and minimum provision for 2013; and one which will continue to grow. Average growth in UK schools is estimated as 30% pa.

Downstream bandwidth requirement				
School	**Devices**	**2012 connection**	**2015**	**2017**
Secondary	400	80Mbps	176Mbps	297Mbps
Primary	40	8Mbps	18Mbps	30Mbps

The above figures are neither overstated nor unrealistic on an international basis. A report by the US State Educational Technology Directors Association (SETDA), *The Broadband Imperative*, recommends at least 100Mbps per 1000 students and staff in 2014-15 for US schools, rising to at least 1Gbps per 1000 pupils and staff by 2017-18.[19]"

More advice on school broadband and internet connectivity is available in NEN Information Sheet 1, *School broadband requirements*.[20]

[19] http://www.setda.org/priorities/equity-of-access/the-broadband-imperative/
[20] http://www.nen.gov.uk/files/NEN_InfoSheet_1_School_Broadband_Requirements.pdf

Appendix 1: Example BYOD policies and agreements

BYOD PARENT/STUDENT USER AGREEMENT[21]

Purpose:

Many students' lives today are filled with media that gives them mobile access to information and resources 24/7. Outside school, students are free to pursue their interest in their own way and at their own pace. The opportunities are limitless, borderless, and instantaneous. In an effort to put students at the center and empower them to take control of their own learning, Booker T. Washington will allow students to use personal technology devices. Students wishing to participate must follow the responsibilities stated in the Acceptable Use Policy as well as the following guidelines.

Device Types:

For the purpose of this program, the word "device" means a privately owned wireless and/or portable electronic piece of equipment that includes laptops, netbooks, tablets/slates, iPod Touches, cell and smart phones. No gaming devices are allowed (to include: Nintendo DS, PlayStation Portable PSP, etc.

Guidelines:

1. Any student who wishes to use a personally owned electronic device within Booker T. Washington High School must read and sign this agreement, get your parent to read and sign the agreement, get it notarized and submit to the building principal.

2. The student takes full responsibility for his or her device and keeps it with himself or herself at all times. The school is not responsible for the security of the device.

3. The student is responsible for the proper care of his or her personal device, including any costs of repair, replacement or any modifications needed to use the device at school.

4. The school reserves the right to inspect a student's personal device if there is reason to believe that the student has violated Board policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device.

5. Violations of any Board policies, administrative procedures or school rules involving a student's personally owned device may result in the loss of use of the device in school and/or disciplinary action.

6. The student complies with teachers' request to shut down the computer or close the screen.

7. Personal devices shall be charged prior to bringing it to school and shall be capable of running off its own battery while at school.

[21] Booker T. Washington High School, USA http://www.btwash.org/BYOD_Report.pdf & http://www.btwash.org/BYOD%20Brochure%20Final.pdf

8. The student may not use the devices to record, transmit or post photos or video of a person or persons on campus. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a teacher.

9. During school hours the student should only use their device to access classroom related activities.

10. The student will use the guest wireless network. Use of 3G & 4G wireless connections is not allowed.

As a student I understand and will abide by the above policy and guidelines. I further understand and will abide by the above policy and guidelines. I further understand that any violation of the above may result in the loss of my network and/or device privileges as well as other disciplinary action.

As a parent I understand that my child will be responsible for abiding by the above policy and guidelines. I have read and discussed them with her/him and they understand the responsibility they have in the use of their personal device.

Device:_____

Serial number:_____

Student's signature: _____

Date: _____

Parent's signature: _____

Date: _____

Items to Include in an Acceptable Use Policy for BYOD[22]:

- A list of any devices that won't be allowed
- A waiver of liability (so school and district aren't responsible for the device being lost or stolen)
- A discussion of teachers' roles, making clear that teachers are not the tech support for every gadget
- A delineation of parents' roles
- A separate BYOT agreement listing specific rules for use (at Forsyth, students and parents must adhere to the Student Code of Conduct, plus Internet Acceptable Use Policy and Internet Safety Policy, plus must initial every item on a list of BYOT instructions)

Some rules might include:

- no use of devices during tests
- must be in silent mode while on campuses and in school buses
- no non-instructional use, such as texting or making or receiving personal calls
- not to be used for taking photos or videos of others on campus during school hours/activities
- non-educational games should not be brought to school; student will use only appropriate applications
- no use of 3G/4G networks in school
- no attempts made to bypass school's network filters
- no hacking of school sites
- no sharing of devices without written parent permission
- devices will run on their own batteries and be charged prior to bringing to school
- transmission of bullying material or material of a sexual nature will not be tolerated
- use of BYOT prohibited in cafeteria, gym, locker rooms, hallways, bathrooms
- consequences established, such as loss of network and/or technology privileges
- district has right to collect and examine any device suspected of being source of attack/virus infection

[22] From *One-to-One 2.0: Building on the "Bring Your Own Device" (BYOD) Revolution*
http://www.samsung.com/us/it_solutions/innovation-center/downloads/education/white_papers/One-to-One_2.0_-_Handbook.pdf

Appendix 2: Sources of further advice

NEN Technical Strategy Guidance Note 5: Bring your own device
http://www.nen.gov.uk/files/NEN_Guidance_Note_5_BYOD.pdf

Yorkshire & Humberside Grid for Learning: Bring your own device
http://www.yhgfl.net/Priorities/BYOD

CESG draft BYOD advice
https://www.gov.uk/government/publications/bring-your-own-device-guidance

Alberta Education: Bring your own device: a guide for schools
http://education.alberta.ca/admin/technology.aspx

Booker T. Washington High School, USA: Bring Your Own Device
http://www.btwash.org/BYOD_Report.pdf

Otago Girls' High School, New Zealand: Considerations for BYOD (Bring your own device to school)
http://www.otagogirls.school.nz/files/downloads/BYODConsiderations.pdf

SecEd: BYOD in 10 steps
http://www.sec-ed.co.uk/best-practice/byod-in-10-steps

YOTS: Your Own Technology Survey
http://www.yots.org.uk/

Hanover Public School District: BYOD
http://byod.hanoverpublic.org/

Online Colleges: Going BYOD (infographic)
http://www.onlinecolleges.net/2012/08/06/going-byod/

Supplier information – BYOD:

CDW-G: Bring Your Own Device: Preparing for the influx of mobile computing devices in schools
http://www.edtechmagazine.com/k12/sites/edtechmagazine.com.k12/files/111331-wp-k12-byod-df.pdf

CDW-G: Bring Your Own Device: Adapting to the flood of personal mobile computing devices accessing campus networks
http://www.edtechmagazine.com/higher/sites/edtechmagazine.com.higher/files/108532-wp-hied-byod-df.pdf

Cisco: BYOD in education
http://www.cisco.com/web/strategy/education/us_education/byod.html

Cisco: Schools Plug Into BYOD: Mobile Devices Transform Learning at Katy Independent School District, USA
http://www.cisco.com/web/strategy/education/katy.html

Dell/Microsoft: BYOD in Education: A report for Australia and New Zealand
http://i.dell.com/sites/doccontent/business/solutions/brochures/en/Documents/2012-nine-conversations-byod-education_au.pdf

Microsoft: Bring your own device to school
http://blogs.msdn.com/b/education/archive/2012/08/15/microsoft-bring-your-own-device-in-schools-whitepaper.aspx

Meru Networks/Samsung: One-to-One 2.0: Building on the "Bring Your Own Device" (BYOD) Revolution
http://www.samsung.com/us/it_solutions/innovation-center/downloads/education/white_papers/One-to-One_2.0_-_Handbook.pdf

RM: Bring your own device
http://www.rm.com/_RMVirtual/Media/Downloads/Bring_your_own_device.pdf

Supplier information – managed wireless network solutions:

Aerohive
http://www.aerohive.com/solutions/verticalmarkets/education.html

Aruba
http://cloud.arubanetworks.com/k12

Cisco Meraki
https://meraki.cisco.com/products/wireless

Meru
http://www.merunetworks.com/industries/education/index.html

Motorola
http://www.motorolasolutions.com/XU-EN/Business+Solutions/Industry+Solutions/Education/Wireless_LAN_for_Education

Ruckus
http://www.ruckuswireless.com/enterprises/primary-education

Supplier information – mobile device management (MDM) & enterprise mobility management (EMM):

Airwatch
http://www.air-watch.com/industries/education

Cisco Meraki
https://meraki.cisco.com/products/systems-manager

Lightspeed
http://www.lightspeedsystems.com/en-uk/products/mobile-manager/

Maas360
http://www.maas360.com/solutions/industry/education/

NB: the above links are provided for information and illustration only; the inclusion of a link in this list does not imply any endorsement by the NEN, nor does exclusion imply the reverse.