Bring Your Own Device FOR SCHOOLS

Technical risks planning

POCKET GUIDE

Future Classroom Lab
by European Schoolnet

European Schoolnet

BYOD Pocket Guide: Technical risks planning

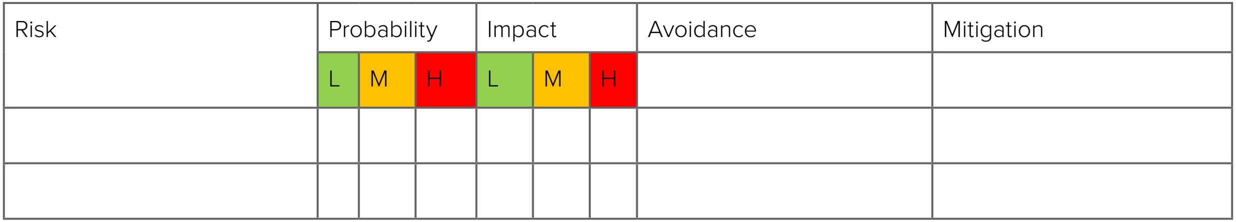
This is one of four shorter 'pocket guides' that has been developed from the full report, Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators that was published by European Schoolnet with support from Acer and the GSMA as part of the work of Ministries of Education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

Related pocket guides that you may find helpful:

- "BYOD Pocket Guide: Technical Advice for School Leaders and IT Administrators". - This pocket guide is an abridged version of the full BYOD Technical Guidelines: Bring Your Own Device for Schools: Technical advice for school leaders and IT administrators.
- "Cloud computing and BYOD" - Using cloud based services in addition to BYOD increases the extent to which students can be both location and device independent.
- "BYOD Pocket Guide: An introduction to the technologies and terminology" - This pocket guide describes some of the technologies required to support BYOD, especially those associated with broadband and wireless networks. It is intended to provide a basic understanding of the technologies and jargon to enable school leaders to take part in informed discussions of key technical issues that will need to be addressed when planning and implementing BYOD.

School leaders and IT Administrators will be familiar with risk management processes involving drawing up and regularly reviewing a risk register similar to the illustration below, listing anticipated risks, how serious they are and how likely to occur, together with plans for how they will be avoided or mitigated.

Figure 15: Risk Register



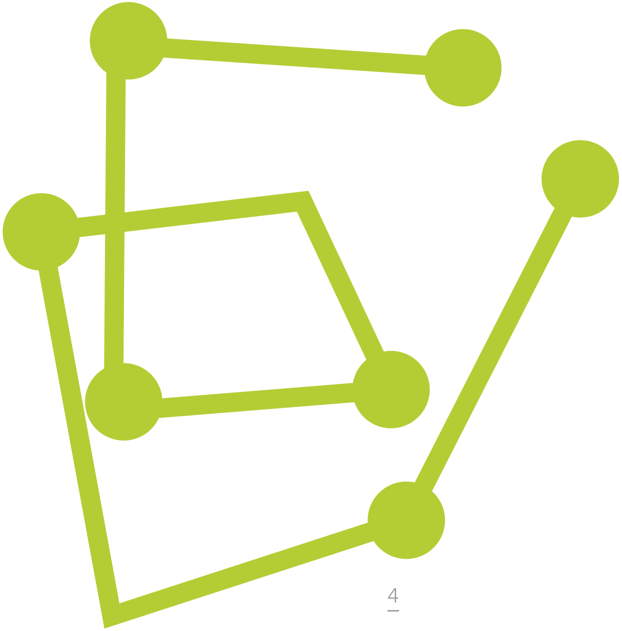
Risk	Probability			Impact			Avoidance	Mitigation
	L	M	H	L	M	H		

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

The technical risks planning matrix in this booklet includes some key risks associated with introducing BYOD and some of the technical options for avoiding or mitigating these. This is not intended to be an exhaustive list of all possible risks and it does not contain non technical strategies (e.g. training, agreed acceptable use policies) for addressing risks which are needed in addition to technical tools and strategies.

School based IT Administrators’ comments on the need for non-technical strategies include:

- Students usually find work arounds when the barriers in place are only technical.
- “No mobiles” policies are almost impossible to enforce in modern secondary schools.
- Stopping students using 3G/4G mobile connections and circumventing school Wi-Fi controls is very difficult. Encourage them to choose to use school Wi-Fi instead. If they get good Wi-Fi subject to sensible but not excessive restrictions for no charge they are likely to save their mobile data for places with no Wi-Fi.



Risk	Who or what might be harmed	Impact	Prevention and/or mitigation options	Pros	Cons
Bandwidth of school broadband connection insufficient.	Users of school IT systems and the implementation of school BYOD policy.	On-line applications very slow, users cannot connect or connection attempts time out. Teachers stop using BYOD devices in teaching.	Upgrade to fastest fibre optic solution available (e.g. 1Gbps FTTC).	Much more bandwidth available.	Cost may exceed budget. May not be available in area. Bandwidth available to end users still low if Wi-Fi equipment not upgraded too.
			Use firewall, proxy server and/or DNS filtering to block student access to bandwidth hungry websites (i.e. those with downloading and uploading of images, sound, video), or limited times when they can access these, and to keep malware and spam off network.	Less bandwidth use, teachers may like “timewasting” websites blocked, increased bandwidth for legitimate traffic.	Blocked websites not available for teaching. Some students may bypass controls with SmartDNS, VPNs or Proxy Servers and continue using large amounts of bandwidth.
			Use traffic shaping to cap bandwidth available to user roles and to applications within roles.	Lower bandwidth usage but applications not completely blocked.	Students may use VPNs to bypass caps.
			Put BYOD students on separate guest-type Wi-Fi network with limited access to the Internet.	Lower bandwidth usage.	Students and their teachers can make only limited use of online resources to support learning.

Risk	Who or what might be harmed	Impact	Prevention and/or mitigation options	Pros	Cons
Wi-Fi network not able to support increased number of users.	Users of school IT systems and the implementation of school BYOD policy.	Students and teachers finding it slow or impossible to connect to Wi-Fi and/or network slow and unreliable.	Carry out, or commission, site survey to check current coverage, capacity and performance of Wi-Fi network alongside estimating future likely number of devices, where and when these will be used.	Vital input to Wi-Fi planning. Where a large Wi-Fi network is new or being substantially upgraded prospective suppliers can be asked to carry out a site survey as part of the tendering process.	Requires good in-house IT expertise or expenditure on external experts.
			Upgrade Wi-Fi network by adding Access Points and/or upgrading to Access Points that support more devices and/or allow dual channel use.	Increased Wi-Fi network coverage and capacity.	Higher capacity access points are more expensive, disruption during installation, may deliver less than desired improvement if there is radio frequency or co-channel interference.
			After adding additional hardware, carry out a post installation validation survey and adjust positioning to optimise performance.	Improved Wi-Fi network performance.	Some effort and disruption and may be additional cost if external experts are used.
			Upgrade to Wi-Fi protocols that support faster data transmission speeds e.g. IEEE 802.11n, IEEE 802.11AC.	Enables achievement of more of the theoretical bandwidth of a high speed broadband connection.	Routers, switches, access points, etc. not compatible with more advanced protocols will need to be replaced. Users with devices that are not compatible will notice less improvement.
			Make sure you know what students and staff are doing and intend to do online with their devices. Review implications for network performance and consider controls listed under broadband bandwidth risk.		

Risk	Who or what might be harmed	Impact	Prevention and/or mitigation options	Pros	Cons
Unauthorised Wi-Fi Access points added to school network.	Users of school Wi-Fi network	Reduces network resources available to authorised users, risk of interference with authorised access points.	The network should include a WLAN controller that monitors access points and will detect any new ones added and not registered.	Improved monitoring and control of access points, improved performance of Wi-Fi network.	If not currently installed, need to be purchased and installed, involving cost and short term disruption to service.
Network accessed by unauthorised users.	Users of school Wi-Fi network and school network and data.	Reduces network resources available to authorised users. May introduce malware or enable unauthorised access to confidential information.	Require all students to enter id and password to access the network and set up profiles for students defining what they are able to access.	Reduces risk of unauthorised users on the network. Easier to identify any authorised user behaving incorrectly on the network.	Time and effort required each year to set up profiles for all students.
			Create whitelist of IP addresses of devices able to connect to the network and only allow these to connect.	Prevents unknown devices accessing the network.	Need to create and maintain whitelist.
			Use Wi-Fi protocol IEEE 802.1X and Radius server to check devices are authorised to connect.	Prevents unauthorised devices accessing the network.	Cost and expertise to implement and manage enhanced security.
Students may access age inappropriate material or unsafe websites while in school.	Students, the reputation of the school and implementation of school BYOD policy.	Students and parents could be upset, students could be harmed, the school could be in breach of their safeguarding responsibilities and might even be sued.	Use firewall, proxy server, DNS filtering and content filtering - possibly including subscribing to a blacklist maintained on behalf of schools - to block undesirable websites and applications.	Reduces risk of students accessing inappropriate or unauthorised websites.	Requires IT expertise but some of these methods will already be in use in schools prior to BYOD.

Risk	Who or what might be harmed	Impact	Prevention and/or mitigation options	Pros	Cons
Students accessing inappropriate material from online services using SSL encryption e.g. Google, Facebook, YouTube.	Students, the reputation of the school and implementation of school BYOD policy.	Students and parents could be upset, students could be harmed, the school could be in breach of their safeguarding responsibilities and might even be sued.	Use Google SafeSearch, YouTube Kids iOS and Android apps and Restricted Search option on YouTube website.	Most inappropriate material will be blocked.	Some inappropriate material may not be stopped by these tools.
			Adding or activating SSL interception/inspection functionality in school filtering solutions.	Will allow inspection of, and if necessary block, material protected by SSL encryption.	Requires technical expertise and requires a security certificate to be deployed onto all student devices .
Students using technical tools to bypass IT Administrator restrictions.	Users of school IT systems, students, the reputation of the school.	Bandwidth available for other users could be reduced, students may be accessing age inappropriate material.	Blacklist IP addresses of VPNs and proxy servers being used by students and block ports typically used by VPNs.	Stops students using specific proxy servers and VPNs to bypass school controls.	The risk is unlikely to be permanently removed if technically literate students switch to alternative tools.
			Involve the students with the best technical skills in this area in helping to police the network.	The students know how they would try to get around controls. Recognises their skills, encourages them to use them responsibly and enhances their CV.	Need to identify the best students to involve and get school leadership agreement to the incentives given.

Future
Classroom Lab
by European Schoolnet

Bring Your Own Device for Schools

Pocket Guide: Technical risks planning

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

BMB Bundesministerium für Bildung

direção-geral da educação

DZS Dům zahraniční spolupráce

HITSA Information Technology Foundation for Education

INDIRE ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

educa.ch

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse

PDST Professional Development Service for Teachers | An tSeirbhís um Fhorbairt Ghairmiúil do Mhúinteoirí

T.C. MİLLÎ EĞİTİM BAKANLIĞI

THE NORWEGIAN CENTRE FOR ICT IN EDUCATION

acer

GSMA

http://fcl.eun.org/icwg

futureclassroomlab europeanschoolnet #FCL_eu