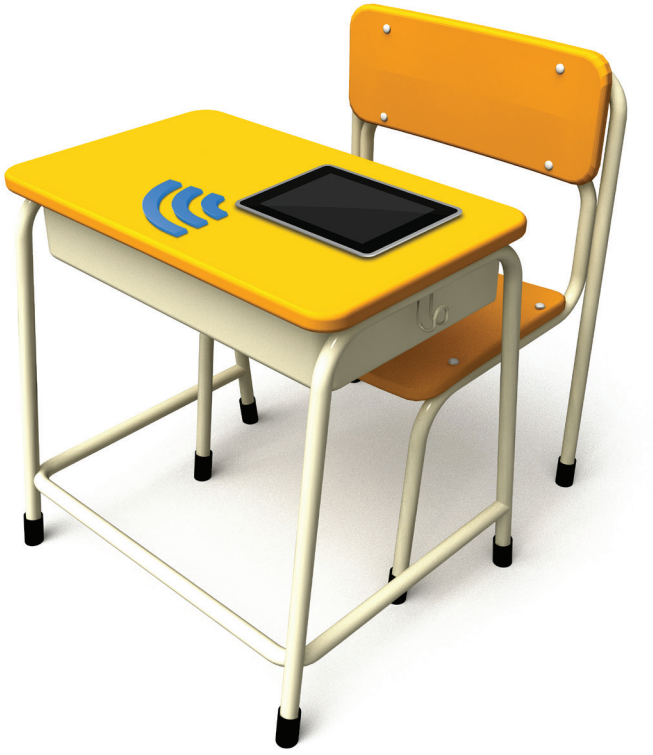
SOPHOS
Security made simple.



Bring Your Own Device

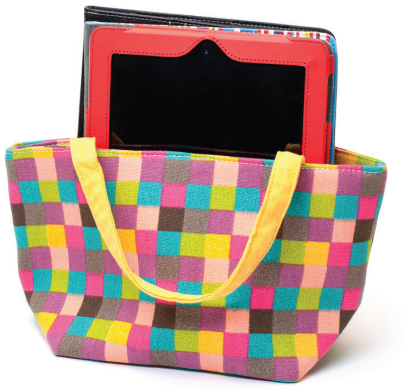
What does it look like for the Education Sector?

With the mass proliferation and increased capability of mobile devices such as smartphones, tablets, netbooks and laptops, many organisations are looking at ways in which they can implement a Bring Your Own Device (BYOD) strategy.
This whitepaper looks at what needs to happen to successfully implement a BYOD strategy in education, but not to look at whether it will improve learning outcomes.

Because users have different needs and their requirements vary across different layers of education, there is no, simple, one-size-fits-all solution. For the purpose of this paper, education can be split into two distinct areas.

1 **Schools (Primary and Secondary) and Colleges**

2 **Higher Education**



Schools

There are two distinct areas within schools; staff and students using their own devices. Students, typically, need to access the internet, this could be via a virtual learning environment, or general, learning-based, web browsing. If a school is allowing students to use their own devices they should be providing wireless network facilities, ensuring students authenticate with their credentials and apply their normal web-filtering rules, as if they were accessing the internet from a school desktop. This can be done via a transparent proxy. Some schools may also wish to provide access to a virtual learning environment, and in this case, virtual desktops are ideal.

Staff will have greater requirements as they need access to core parts of school networks. If staff members are to use their own device, they will need to accept a degree of management. This may be allowing a sandbox environment to be installed on a device, to keep personal and work data separate, although this can be intrusive on devices and affect performance. Alternatively, it could be to allow a level of management in terms of security rules such as password strength and ensuring any built-in security is enabled. Both methods have advantages and disadvantages, and the approach is really a decision for the school's leadership team to take.

These solutions are most appropriate for smartphones and tablets. Some organisations also allow staff or students to use their own laptops. In these cases, schools need to be able to assess the security settings of the device before it connects to a network, even if it is configured to only allow internet access. Some form of network access control should be implemented so that security policies can be ensured to protect the integrity of the school network.

Staff usually have access to sensitive data, such as pupil records. So schools need to ensure this data is secure. At the very least, there needs to be an acceptable use policy that states that encryption needs to be used to protect personally-identifiable information. This is sensible, not only for security, but also from a reputational point of view. As parents have greater freedom to choose the school their children attend, schools need to minimise the potential impact of negative publicity from data breaches which can seriously affect close communities. Therefore, if schools have the ability to check the content of the data being accessed on a personal device, they can then put policies in place to protect this data, and at least prompt the encryption of sensitive data; if not completely block the transfer of sensitive information.

Higher Education

Higher Education users tend to be savvier than those at schools, and have high expectations of what they should be able to use their devices for, and less willing to accept restrictions on use. They also have a far greater use of data, especially if the university conducts sensitive research. Universities also have the added complexity of a large number of users, with tens of thousands of users and hundreds or thousands of staff.

As with schools there is a degree of user separation. Undergraduate students would typically require wireless access with little or no filtering applied. Generally they do not have access to sensitive information at this stage of their university career. Universities may look to limit bandwidth usage for less critical applications or to restrict the use of bandwidth consumption on file sharing services.

Post graduates and staff will have different requirements. The management of an unknown number of disparate and rapidly-evolving devices can cause problems. In this case it makes more sense to protect and manage the sensitive information rather than the personal device. It's possible to allow access to sensitive information on mobile devices, providing the data is encrypted and policies are in place to manage it. This is far easier than to manage a constantly-changing array of personal devices. However, it is important to maintain management of devices accessing the university network. They need to be checked to ensure their security has not been compromised, either by being jail broken or by having some security features disabled. This means a form of management for smartphones, or network access control for laptops, etc.

Contact the Education Team

Tel 01235 465935
Email education@sophos.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

SOPHOS