PROCAT

PROSPECTS COLLEGE OF ADVANCED TECHNOLOGY

CASE STUDY

Implementing a Bring Your Own Device (BYOD) policy

Commissioned and funded by

The Education & Training Foundation

Implementing a Bring Your Own Device (BYOD) policy

CASE STUDY

1: CONTACT DETAILS

Name: Neil Warren

Role: Chief Operating Officer

Email: neil.warren@procat.ac.uk

2: WHAT DID YOU SET OUT TO DEVELOP AND WHY?

Student feedback, captured through a series of face-to-face forums and a student survey conducted in 2015, highlighted the need for the college to increase the IT access and capacity for learners. Whatever we put in place needed to ensure sustainability and achieve equality of the digital environment inside and outside college.

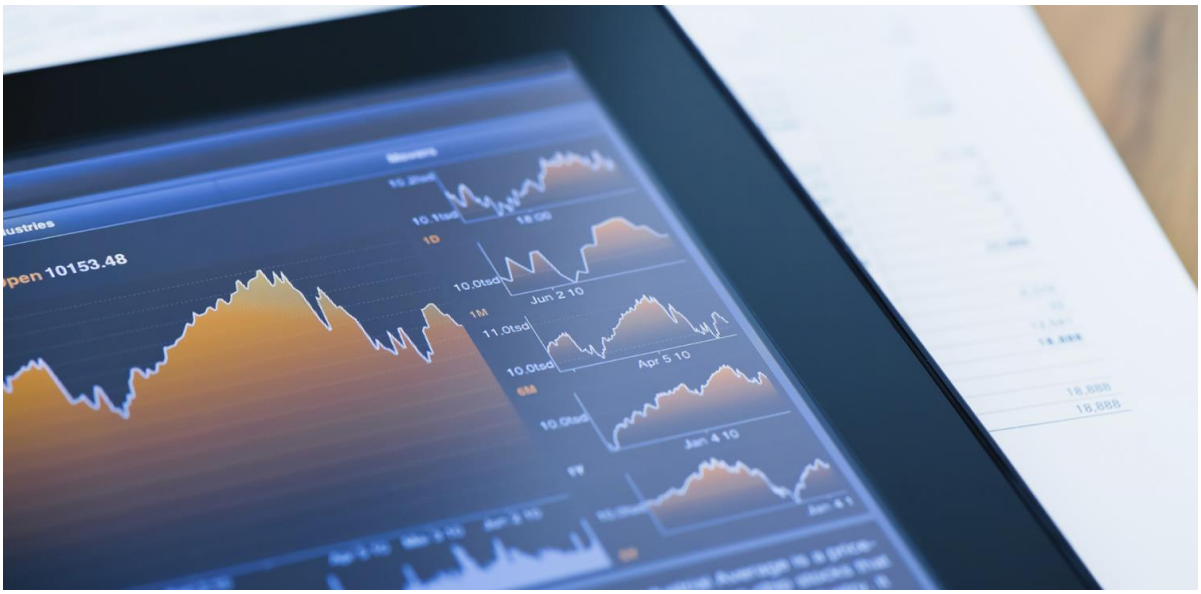
As 97% of our students own a smartphone and 82% a laptop the solution to this challenge was seen to be the implementation of a BYOD policy which was introduced in September 2015.

3: THE PROCESS – WHAT DID YOU ACTUALLY DO?

As soon as it was agreed by the senior leadership team that we would go ahead and introduce BYOD we turned to address practical considerations relating to IT infrastructure, security, filtering, management and eSafety by:

- establishing a BYOD network that is separate to the college network;
- providing a network that is completely open with the exception of illegal sites which are blocked using 'smoothwall';
- ensuring that students who wish to use their own device download specific software so that policies on internet safety and anti-virus software are followed;
- summarising the BYOD policy in poster format around the college;
- controlling download speeds to protect network performance.

We also made sure that students who do not have their own device are able to book the use of a laptop or use machines within the learning resource zones based at each campus.



4: WHAT DIFFERENCE HAS THIS MADE?

Students are now able to use their own devices to access the college network for their ePortfolio, core learning resources and documents. Staff encourage the students to use their phones during sessions to, for example conduct research, access information via applications such as QR codes and capture evidence for their ePortfolios in the form of photographs and videos.

Across an average 5-day college week 866 student users will access the BYOD network (i.e. 50% of the student population) using an average of 424 GB of data. There has undoubtedly been usage transfer – a lot of the traffic has been diverted from G3/4 networks to the BYOD WiFi network. It might be seen that we as a college are bearing the cost of something the students provided for themselves. However this is a real benefit to students and brings them onto our network which they will also use in their studies.

Encouragingly there has been very little misuse or abuse of the network (it is clear in the policies that misuse would result in this privilege being withdrawn).

5. LESSONS LEARNT

The introduction of the BYOD policy has gone remarkably smoothly however by completing this process we have learnt some valuable lessons such as the importance of:

- planning your service set identifiers (SSIDs) and the authentication requirements for each of them. Separate each SSID onto its own virtual local area network (VLAN);
- ensuring your filtering is finalised and tested before going live as it's easier to make changes then;
- considering access points (AP). We've had to move APs to other locations to give more coverage in "hotspots" such as student self-study areas;
- rotating guest SSID (Wireless Networks) passwords; passwords are often spread and students find them out;
- resourcing a member of staff to monitor any web filtering processes that you put in place and to take action as appropriate, software alone does not do this job for you.

If you are considering introducing BYOD here are our top five tips.

1. Make sure all users are kept fully informed throughout the process about what is going to be introduced, when and why as well as how this will affect them.
2. Have clear policies regarding use/misuse of the BYOD network.
3. Ensure security is watertight and that the rest of the infrastructure can cope with the additional traffic.
4. Plan your access point locations to ensure good coverage across all areas of the site.
5. Make sure you have tiered bandwidth limits on the "non-company" SSIDs (Wireless Networks), Guest network, student BYOD, staff BYOD.

6. RESOURCES

PROCAT's BYOD Policy

The policy links to other key PROCAT policies relating to information technology, eSafety and data protection.