

Winter 2016

www.medhurst-it.com



We've moved!

We're now located at our new larger offices just up the road at:

17 Brunel Way
Segensworth East
Fareham, Hampshire
PO15 5TX

With five times more space than our previous offices and lots of parking, we will be able to carry an even larger selection of products for your convenience.

Our phone number: **01489 563000** and primary email address: **sales@medhurst-it.com** remains the same. Since we first opened our doors in 1986, your loyal business and support is one of the main reasons why we've grown so much over the years. We look forward to welcoming you to Brunel Way very soon!

Pre-loved PCs



Microsoft
AUTHORIZED
Refurbisher

Working PC base unit from
£3 per month with warranty

The usable life of a typical computer is up to seven years. Considering a 'Pre-Loved' computer makes financial sense for schools and colleges.

New cars lose 20% of their value the moment they leave the showroom. It's worse for computers. Big businesses change their computers every three years injecting a large supply of perfectly usable computers back into the PC market. When it comes to researching online, word processing and standard student workloads, you don't need the latest spec.

Medhurst is one of the largest suppliers of second hand computers in the UK. With a three year warranty and typically costing less than half the price of a new one, refurbished computers are an attractive alternative.

Various specifications available.
Please call us for your exact requirement.

We're already planning for Bett 2017 - have you registered yet?



We'll be back at the leading education technology show on **25-28th Jan 2017** on **stand G270** helping teachers to transform their educational environments and improve productivity at their schools.

With over 450 clients in education across the UK, we provide cost-effective and future-proofed IT solutions through our partnerships with Hewlett Packard, Hewlett Packard Enterprise, Aruba a Hewlett Packard Enterprise Company and Microsoft.

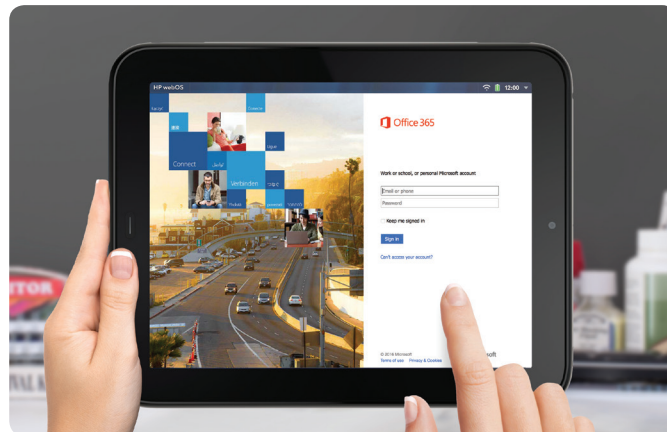
This year on the Medhurst stand, visitors will see a live working environment of HPE servers and storage, Aruba switching and wireless, all using Microsoft System Centre and Veeam backup solutions.

We'll also be demonstrating the latest version of our Dashboard cloud and remote working solution for schools, enabling them to deliver their software applications to all students and staff whether on or offsite, ensuring secure access to any application, anytime, anywhere.

In the meantime you can join in the weekly **#BettChat** on Twitter every **Tuesday at 4.30pm** to debate and discuss the most pressing matters in education today.



Microsoft becomes first global provider to deliver complete cloud from UK data centres



Microsoft has begun a roll-out of its cloud services from data centres in the UK, bringing to an end the former requirement for its customers to accept that their data be hosted in Ireland or Amsterdam in order to qualify for EU residency.

Azure and Office 365 services are now available from locations in London, Durham and Cardiff.

The UK residency opens up the possibility of new contracts in the public sector, and complies with UK data protection laws. Azure and Office 365 is built on Microsoft's cloud principles of security, privacy, compliance, transparency and availability.

It is expected that educational institutions will embrace the elastic and scalable services that Azure and Office 365 can provide as an alternative to managing and supporting their own in-house hardware. Microsoft hopes to create opportunities for innovation and help every student on the planet achieve more.

"As one of the largest cloud operators in the world, we've invested billions in building a highly scalable, reliable, secure, and sustainable cloud infrastructure. With the introduction of new regions in the UK, Microsoft has now announced 34 Azure regions around the world with 28 generally available today – more than any other major cloud provider."

Azure's Partner Director Tom Keane

250,000 staff at the UK Ministry of Defence will be using the UK-based services, along with existing customers such as Aston Martin. Other customers moving to the UK services include Britain's largest health trust, the South London & Maudsley (SLAM) NHS Trust.

Microsoft has the broadest set of compliance certifications of any public cloud provider.



smoothwall

The UK's #1 web filtering solution for schools

We are pleased to announce that we are working with Smoothwall to offer our education clients innovative internet security and web filtering solutions to make the internet a safe place for children to learn and explore. The Smoothwall solution also helps schools keep up with an ever-changing legislative burden and protect their users.

The Smoothwall solution meets all of the functionality set out by the revised statutory safeguarding guidance for schools and colleges 'Keeping children safe in education' released by the Department for Education. This revised guidance commenced in September 2016 and states that it is essential for children to be safeguarded from potentially harmful and inappropriate online material, such as abuse, substance misuse, bullying and radicalisation. Governing bodies and proprietors must therefore now not only ensure they have the most appropriate 'web filtering' in place but also the appropriate 'monitoring' in place.

In collaboration with Smoothwall, we have a whitepaper available to demystify the facts around online safety and take a closer look at how Smoothwall can help schools with regard to appropriate filtering and appropriate monitoring, which is featured heavily as part of the new legislation. Contact the Medhurst Education team on 01489 563000 or via email on education@medhurst-it.com for your copy of 'Keeping Children Safe in Education'.

Smoothwall Key Features:

- Content aware analysis - Smoothwall identify brand new content on the web in real-time, long before URL blocklists
- Easily build filtering policies based on user, content, time and location
- Flexible tools to allow read-only access, block social gaming or remove inappropriate content
- Filter guest mobile devices on your network
- Safeguarding reporting suite - analysing internet activity against a number of safeguarding categories including radicalisation, suicide and abuse.
- Over 300 custom report formats
- Anonymous proxy blocking

Smoothwall is a member of the Internet Watch Foundation and implement the CAIC list of domains and URLs. Smoothwall also implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

To find out more about the UK's #1 web filtering solution for schools, contact us today



Follow us:



twitter.com/medhurst_it



linkedin.com/company/medhurst



Special Manufacturer Relationships

Medhurst has been partners with Hewlett Packard for eight years now, working with them to offer both staff and students at schools total access to next-generation content, curricula and resources via a secure, cloud-enabled, mobile-friendly infrastructure.

Last year, Hewlett Packard split into two companies: HP Inc, suppliers of PCs, tablets, laptops and printers and HPE (Hewlett Packard Enterprise) suppliers of servers, storage, switching and wireless solutions. HPE also acquired leading wireless solution provider Aruba, manufacturers of mobile-first, cloud-first business apps.

As an HPE and HPE Aruba accredited partner, we are able to secure the best prices and warranties for your hardware devices and can offer schools access to exclusive HPE promotions and discounts.

If your school needs an IT refresh, call us today to see how Medhurst, Hewlett Packard Enterprise and Aruba a Hewlett Packard Enterprise Company can transform your learning environment.

Our partners and accreditations



Hewlett Packard Enterprise



Microsoft



The three most common IT security threats that you should be prepared for...

Phishing Attack

1

What happens:

In November 2013, the UK's National Cyber Crime Unit warned of a mass email-spamming event targeting tens of millions of UK customers – predominantly small and medium-sized businesses.

The emails carried an attachment that appeared to be linked to the correspondence in the message, for example a voicemail, fax or details of a suspicious transaction or invoice.

The attached file was actually a piece of malware called CryptoLocker, which caused massive disruption to its victims by encrypting files and then demanding a ransom to unlock them. While CryptoLocker is one of the most infamous pieces of malware delivered via this type of attack, every month, thousands of businesses fall victim to email attachments that lead to serious network and system compromise.

How to avoid it:

Investing in an Anti-Spam solution to provide protection from email-based attacks is a “quick win” for security-conscious IT professionals and would address most security incidents resulting from user interaction with email. But training staff to be vigilant should be considered equally important.



Brute Force Attacks

2

What happens:

Brute Force attacks – either from malware looking for its next host to infect, or a malicious actor running a script – generally target a single service exposed to the Internet, such as Remote Desktop, VNC, Outlook Web Access or SMTP services. Attacks consist of a predictable and systematic checking of all possible passwords until the correct one is found. This then grants access to the network, in many cases with domain administrator privileges. At this stage it's unfortunately game over for the defenders.

How to avoid it:

Your first point of call is to look at implementing robust complex passwords for all Internet-facing services and managing those passwords accordingly. Alternatively, you could move them to a hosted cloud provider that has multiple ISPs and DDOS mitigation.

Distributed Denial of Service (DDOS)

3

What happens:

In late 2014/early 2015, both the PlayStation Network and Xbox Live went down after a group called LizardSquad began using a tool called LizardStresser to attack their network connections. LizardStresser leveraged poorly secured routers that had default passwords. As a result, thousands of routers were turned into internet-facing cannons that blasted Internet traffic at the IP addresses critical to the gaming networks. In a sinister twist, cybercriminals may try to extort money from a potential victim – threatening them with a DDOS attack if they don't pay.

How to avoid it:

There are a range of options for organisations that may be at risk of either DDOS extortion or DDOS attacks. Most importantly, if there are Internet-dependent critical systems they should not be located on premise, they should be in a data centre with multiple Internet providers and infrastructure redundancy. Medhurst and Microsoft Azure have excellent Internet connections, DDOS mitigation capability and a redundant infrastructure.