“Some of our staff do quite a lot of work outside of the Trust. There was a lot of frustration for users unable to connect across the VPN to us, because we would have to tell them to come into the Trust and we’d fix it there. That wasn’t always feasible for some people.”

DAVID MARSHALL, HEAD OF IT

Birmingham Women’s and Children’s NHS Foundation Trust

Officially launched in February 2017, Birmingham Women’s and Children’s NHS Foundation Trust united Birmingham’s Children’s Hospital and Birmingham’s Women’s Hospital together under one NHS Foundation Trust. The first of its kind in the UK, the Trust comprises around 6,000 staff providing pediatric and maternity services, plus much more, to thousands of patients in Birmingham, the West Midlands and beyond.

The need to provide better support to remote staff

As a small team, the IT support function for Birmingham Women’s and Children’s NHS Foundation Trust needs to be able to provide assistance in a quick, efficient, and secure way. Issues with providing support to remote staff that were connecting to the network from home via VPN, particularly on smart devices such as tablets, had been a challenge for many years. There was no mechanism in place to support these users, without having them return on-site to the Trust with their device to have their issue addressed. For many remote workers, some of whom were working long distances from the Trust, this just wasn’t a practical solution.

A further problem was having the ability to accommodate third parties or contractors who required access to the Trust’s network. It was essential that Birmingham Women’s and Children’s NHS Foundation Trust maintained absolute control and oversight of third party access, only granting entry to the necessary systems and data.

Crucially, any new technology solution implemented to address these challenges needed to be totally secure. By the nature of its work, the Trust and its staff handle incredibly sensitive information and are accountable under regulations including the Data Protection Act, the new General Data Protection Regulation and local governance policies. A system that guaranteed compliance and provided robust, centralised audit trails that could be reviewed in real time for all activity on the network was vital.

Bomgar’s Secure Access solutions save time for both support staff and end-users

The Birmingham Children’s Hospital had been a Bomgar customer for many years before the merger, so the Trust selected Bomgar’s Remote Support and Privileged Access products across the merged organisation.

Now, whenever an off-site member of staff is having trouble connecting to the Trust’s networks, support can be given instantly and remotely. So long as the user has internet connectivity, expert staff can access the device, take control and immediately reconfigure it to access their VPN securely. This has saved time for both end-users and staff, as the team can troubleshoot connection issues remotely, instead of requiring people to come into the Trust to have their devices configured.

Crucially, the Remote Support solution works across multiple devices and operating systems. This is especially important as many of the Trust’s staff rely heavily on portable tablet devices, which are becoming the platform of choice in delivering the services the Trust offers.
For example, Forward Thinking Birmingham, the city’s mental health partnership for ages 0-25, use around 300 Samsung tablet devices to help them support children and young people. Apple iPad devices are also increasingly used on pharmaceutical delivery trolleys in hospitals, using Bomgar Jump Clients to enable quick and secure support when needed within the hospital environment.

The Trust also depends on numerous third-party suppliers and other NHS organisations to deliver its services. This is where Bomgar’s Privileged Access solution has been critical to ensuring compliance in that they must manage and audit the access suppliers have to its systems. For third-parties, like the University Hospital of Birmingham, it allows the Trust to define different permission levels and grant them secure, easy access to just the systems and data they need.

Maintaining secure access at all times

There was some initial pushback to the new Bomgar relationship – the Trust already used other products such as SCCM to provide remote support – and some questioned the need to implement another solution. However, since installing Bomgar’s Remote Support and Privileged Access solutions, the support team has seen massive improvements in the way it provides support to the rest of the Trust and delivered cost savings. Crucially, it has improved the efficiency and speed of dealing with end-user issues, which, for a small team needing to make the best use of its time, has been an enormous benefit.

The end-users themselves are also pleased with the support they are receiving. Using the questionnaire functionality of the solution, the support team has received great feedback from those satisfied with the service.

Overall, Bomgar’s Privileged Access and Remote Support solutions have allowed the Trust to keep its network secure and compliant whilst delivering an improved service to its staff and quickly enabling its third parties to access its systems. Through granular control of who has access to what on the network, the Trust can ensure that all of its sensitive data is secure and only accessible to those who should be able to see it.

**ABOUT BOMGAR**

Bomgar is the leader in Secure Access solutions that empower businesses. Bomgar’s leading remote support, privileged access management, and identity management solutions help support and security professionals improve productivity and security by enabling secure, controlled connections to any system or device, anywhere in the world. More than 12,000 organizations across 80 countries use Bomgar to deliver superior support services and reduce threats to valuable data and systems. Bomgar is privately held with offices in Atlanta, Jackson, Washington D.C., Frankfurt, London, Paris, and Singapore. Connect with Bomgar at www.bomgar.com.