

Islington Council Case Study

Islington Council meets austerity measures and provides flexible working with Becrypt solution

Council implements Becrypt Trusted Client to enable secure remote access to network and facilitate cost reduction strategy

Islington Council is an inner London borough in north London that has been Labour-controlled since the May 2010 local elections. The council's key aim is to achieve a fairer Islington – while the borough is geographically small, Islington's population is diverse.

It is home to some of the wealthiest people in the UK living in some of the most desirable neighbourhoods in the capital. However, it is also home to real poverty and deprivation and is officially the 14th most deprived local authority in England.

Meeting the austerity challenges

Today Islington is being hit harder than any other London borough by government cuts – the council has to save around £100million between 1 April 2011 and 31 March 2015. To meet these challenges the council is working in partnership with Becrypt to provide Becrypt's [Trusted Client](#) solution to the 3000-strong workforce, enabling its employees to work remotely and securely access the council's network.

The partnership will help the Council realise its drive to cut costs through estate rationalisation and co-location – it will enable staff to work from any department, in any office, with no disruption to their productivity.

Secure remote access to council data

Trusted Client provides secure remote working and data encryption for the council's employees. Trusted Client gives highly secure, low cost, mobile access from any unmanaged, internet enabled PC, laptop or thin client device used in any location. It is the only solution of its type on the market that has full CESG accreditation for the handling of data up to Impact Level 2 (which covers all of Local Authority level data).

Trusted Client transforms an unmanaged PC or thin client into a secure network access point. It is also very portable and easy to implement - either carried on a USB stick or installed directly onto a PC or thin client.

Using Trusted Client the user reboots the device and a secure isolated environment is created, enabling them to access the corporate network, data and applications. Only the host machine's memory, processor and keyboard are used, so the council network is protected from malware and any data that is accessed is encrypted. When the system is shut down, the volatile memory is cleared leaving no trace of the session.

Providing flexible working

Using Trusted Client, Islington Council is enabling flexible working for staff and is also fulfilling its social inclusion policy. Furthermore, the solution offers an attractive option for staff who may be reluctant to take council laptops home with them either through fear of losing or damaging them, or simply because they are too heavy to carry. The lightweight but robust key-fob form factor of Trusted Client means that staff can plug it into their own home PCs with no risk of virus infection or cross-contamination.

"Trusted Client was the knockout product of Infosec 2009, and it ticked a lot of boxes for us: being the only fully accredited CESG solution of its type, it enables us to fulfil our security obligations, while ensuring that we can accommodate our employee's flexible working requirements," said Adrian Gorst, Head of ICT Service Delivery, Islington Council. "Becrypt had the only solution which provided the functionality and security we needed, while remaining cost effective."

Ensuring business continuity

By using Becrypt's Trusted Client solution, Islington Council also supports its business continuity plan, which translates into a significant return on investment. For example, should staff be kept away from work due to transport problems, adverse weather or because of a sick child, they can carry on business as usual by plugging the Becrypt device into their home PC. In financial terms, this single day of productivity will cover the cost of Trusted Client, a real advantage in today's tough economic climate. The CD/DVD device is performed by Media Client, so there is no requirement for third party CD/DVD burning software.

For more information please visit www.becrypt.com

Headquarters: Becrypt Limited, 90 Long Acre, Covent Garden, London, WC2E 9RA, United Kingdom Tel: +44 (0) 207 557 6502 Fax: +44 (0) 207 557 6599

United States: Becrypt Inc, 1600 Tysons Boulevard, 8th Floor, McLean, Virginia 22102, USA Tel: +1 (877) 221 7775 Fax: +1 (703) 245-3001

Australia: Becrypt Pty, Level 12, 1 Pacific Highway, North Sydney, NSW 2060 Tel: +61 (0) 2 9959 1961 Fax: +61 (0) 2 9959 3003