COUNCIL 15 JULY 2015

MOTION ON NOTICE – ICT: BRING YOUR OWN DEVICE

"To improve the IT (email and intranet etc..) service offered to Councillors and reduce costs this council is to investigate a form of byod (bring your own device) with a platform-independent remote access solution for this communication such as that used in many neighbouring councils, such as Fylde, Lancashire County Council, South Lakes, and Cumbria.

This council requests that the Head of IT reports to Budget and Performance with his costed findings as soon as possible, and at the latest by the October meeting."

The aim is to improve the usability to the councillor group, to reduce costs, improve efficiency, and aim towards the stated aspiration of the Chief Executive of a paperless council. It would incidentally comply with the published constitution Members Allowance Scheme (June 2015), which in para 2.3 says .....Where a member wishes to utilise their own PC or laptop, rather than use a Council provided laptop, this must be the subject of prior agreement with the Council's Information Services Application Manager, and the Council may enable a remote access facility for that Member. This is a position some of us would like, and we have been told is not possible.

Motion to be proposed by Councillor Goodrich, Brookes, Cooper, Caroline Jackson and Phillippa Williamson.

Officer Briefing Note

Background to Bring Your Own Device (BYOD)

Prior to the Public Services Network (PSN) compliance regime, the use of personal devices was allowed through portal access to systems using username, password and second factor authentication (2FA). Subsequently, however, Council Officers were told by the PSN authority (PSNA) that BYOD was not acceptable from any device that came under the scope of PSN compliance. The ICT Manager challenged this at a Vodafone/PSNA event held in Manchester on 31 October 2013, stating that he did not believe that using a portal with 2FA was insecure. He was told by the government information security representatives that in fact any unmanaged device could be compromised and the images being presented on its screen could then be captured and relayed to an unknown destination. Further the project lead for the PSN told him that if the Council made a submission for PSN compliance including any use of BYOD, the submission would be rejected.

Following this the Cabinet Office put out some guidance on BYOD which appeared to say that councils could implement BYOD. However, the Council could not make use of this guidance for two reasons. Firstly, for a device to be covered by the guidance, the detail effectively made it a "buy your organisation a device policy" in that the device would have to be handed to the authority immediately after purchase, so no existing devices could be used, and the authority would then have to apply the same level of management to the device as for any device bought directly by the authority. This makes no sense for either party in that the individual ends up with a device entirely different from what they thought they were buying and the authority has to support a high number of different kinds of devices which is costly and inefficient. The second reason was that due to the way the Council's network had been built up over a period of many years, it was impossible at that time to take any device connected to it out of scope of the PSN. Officers are currently replacing and reconfiguring

the network infrastructure which, by October 2015, will potentially provide a network, where certain sections can be taken out of scope for PSN compliance.

In the latest scheme of provision of computer services for councillors, a choice is given between a laptop, tablet or mini-tablet device. The first two make use of existing Microsoft licences together with additional security devices in the computer room to provide access to resources via a PSN compliant connection to our network, using Wi-Fi connections within councillors' homes. The latter is a low cost device but with mobile connectivity to allow councillors access to emails from anywhere with a mobile signal. The rollout of these devices is well under way but not yet completed.

In context of longer term aims, a paperless environment is aspirational and whilst some progress may be made, it is not yet achievable.

Current PSN Position

On Friday 22 May 2015 at a Local Government PSN Programme Board workshop, the Government Digital Service (GDS) PSN team gave out new verbal guidance on the use of BYOD which amounted to (paraphrased) "Do as much BYOD as you want but don't allow any connection from it to gain access to the PSN".

This, taken with the work being undertaken on our network, would mean that from October, as far as PSN compliance is concerned, we should be able to consider the use of BYOD, subject to there being a sound business case to do so. As usual, this will need a review to be undertaken to demonstrate that the benefits outweigh the costs and that the Council identifies the associated risks and is prepared to accept them.

However, this is still a changing picture. The society of IT management (SOCITM) are in talks with GDS and Officers are hoping for a single set of guidance later on in the year. It is probably not a good idea to look at any options until this guidance has been released.

Additionally, Lancaster City Council has very recently been selected for a PSN compliance audit commencing in August. This is in addition to, and in support of, the normal compliance process. If the Council is seen to be changing its stance on BYOD before it has completed its current security improvement action plan, then there is a risk that the audit may be adversely affected.

Other Councils

Other councils have chosen different ways of providing councillors with access to resources, either: as we do, providing fully managed devices; BYOD with portal access with and without data download to the device; placing all councillor resources in the cloud.

The differences are due to differing ICT strategies, risk appetites, timing of PSN submissions and scoping of their PSN submissions.

Risk and Information Security

There are two general approaches to information security, these being technical security measures, and written policies that individuals sign up to.

Whilst written policies transfer some of the accountability for any security incident, they are dependent on the individuals actually abiding to them and there is evidence of this not happening in the past.

Technical security is only good for devices that the Council has control of and the fact that we are aware of two of our councillors having personal email accounts hacked in the past year would show that there is a potential problem with personally managed devices.

There are a number of risks with the deployment of BYOD with regards to Information Security and Information Management. If full remediation was not introduced for each one of these risks, then the introduction of BYOD would introduce vulnerabilities into Lancaster City Council.

There are a number of guidance notes and legal frameworks that Lancaster City Council complies with. The two most relevant are CESG's Cyber Security Guidance for Business[1] (which includes 10 Steps to Cyber Security) and The Data Protection Act (1998)[2].

For information, the following table sets out a summary of the security and information considerations for the main BYOD approaches currently adopted by councils.

Option	Security	Information
A) Provide fully managed devices while maintaining a view on improved BYOD security and guidance from PSN.	This is a secure option. It allows for the same solution to be used for councillors and staff, thereby reducing support costs. All software licences and devices for this have already been procured.	This gives the best protection to personal and confidential information (Information considered to be OFFICIAL under the Government Security Classifications April 2014[3])
B) Allow BYOD with portal access and no data download or interaction with the rest of the device (commonly referred to as sand boxed)	Requires: investment in virtual desktop infrastructure, portal software, two-factor authentication devices and supporting server and licences. Issues: Due to the fact that Lancaster City Council would have no control over: password access to the device (10 Steps – Managing User Privileges); who uses the device and consequently has access to the data on the device (DPA Principle 7); anti-virus software (10 Steps – Monitoring); patching (10 Steps - Secure Configuration), then there	The key logging and image

	would be a risk that user name and password, together with all key depressions and images of what the councillor has viewed could be intercepted. The loss of user credentials could assist an attack on our network.	capture could result in private and/or confidential information getting into the wrong hands
C) Allow BYOD with portal access and encrypted data download	Requires: as per (B) Issues: as per (B)	Issues: as per (B) plus: on ceasing being a councillor there is no way that we could check for personal data being held on the device so could contravene DPA Principal 7; at end of device life we securely destroy the data but this may not be done on an individual's device (again DPA Principal 7)
D) Place councillor communications in the cloud	This is the most secure option with respect to the council's network. Requires: Additional licence costs and training for ICT support.	Information held in the cloud can be secured to OFFICIAL standard.

Local Cyber Resilience

Threats from the internet are increasing and the DCLG is working to raise understanding of these and how to mitigate them and has recently released Understanding Local Cyber Resilience [4]. The Council would need to consider BYOD in this context.

Platform-independent BYOD

Truly platform-independent BYOD is not available, there are just solutions that can be supported by greater numbers of platforms depending on what you pay for.

Councils that have implemented BYOD with the agreement that the council supports the interface whilst the councillor supports the equipment have had an additional support overhead, partially due to the rapidly changing devices available and the BYOD not quite keeping up to date.

ICT restructure and current workload

ICT have recently had a new structure approved and have a number of vacant posts which are in the process of being filled. There is a program of projects to be delivered this year that is already challenging resources. Any additional work at present would jeopardise this program.

Officer Preferred Way Forward

Benefits and issues of the latest computer equipment supplied to councillors are still not fully understood. Whilst it is appreciated that a form of BYOD could well be more convenient to councillors and deliver benefits to the Council, the timing of undertaking any BYOD review is expected to have a significant influence on the option chosen and might lead the Council going down the wrong (or less than ideal) path. Officer advice and the preferred way forward is therefore that a BYOD review be included in the development of a wider Digital and ICT Strategy, for consideration as part of the 2016/19 Budget and Planning process, rather than a review with costs being prepared by October at the latest. This may result in a few more months' delay, but should provide for a more robust strategy going forward.

References

1. Cyber security guidance for business (Internet). https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility (Accessed 02.07.2015)
2. Data Protection Act 1988 (Internet). http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 02.07.2015)
3. Government Security Classifications April 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf (Accessed 03.07.2015)
4. Understanding Local Cyber Resilience, a guide for local government on cyber threats and how to mitigate them https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf (Accessed 06.07.2015)

S151 Officer Comments

The s151 Officer has been consulted and has no further comments to add.

Monitoring Officer Comments

The Monitoring Officer has been consulted and has no further comments.