LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

SUPPLEMENTARY REPORT

Budget and Performance Panel

Tuesday, 23 February 2016

The following report was marked 'to follow'. It is now enclosed, as follows:

Agenda Item Number	Page	Title
10	1 - 13	ICT - BRING YOUR OWN DEVICE
		Report of the Chief Officer (Resources).

BUDGET AND PERFORMANCE PANEL

Bring Your Own Device (BYOD)

23 February 2016

Report of Chief Officer (Resources) and ICT Manager

PURPOSE OF REPORT
To provide information to the Committee on BYOD, to help inform views regarding value for money of any future BYOD policy.
This report is public.

RECOMMENDATIONS

1. **That the Panel gives its views on the information and issues raised in the report.**

1   Introduction

1.1   Council, at its meeting held on 15 July 2015 (minute 37 refers), resolved "to improve the ICT (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." The aims were to improve the usability to councillors, reduce costs, improve efficiency and aim towards the aspiration of a paperless Council.

1.2   This report follows on from that Council resolution. To provide context and background to the Council's current position, the Council motion and Officer briefing note as prepared back in July are attached at *Appendix A*.

1.3   This report only considers BYOD for councillors, not for staff, to keep matters simpler. The wider application of BYOD is also under review, however.

2   Further Background

2.1   In the April 2013 Lancaster City Council entered into a 3 year agreement with Microsoft under a Government arrangement known as Public Sector Agreement (PSA) 12. This covers all the Council's Microsoft licences and gives some additional utilities such as a product known as Direct Access, which allows the Council to manage devices away from the council network in a secure fashion.

2.2 In 2013/14 the Cabinet Office chose to adopt a zero tolerance approach to PSN compliance, which effectively outlawed BYOD and, unfortunately, because Direct Access was so new and had not been tested by the Government's information security authority (known as CESG), Direct Access was also outlawed. Rather than spending any more time or money on an alternative remote working product, Officers chose to wait for CESG to release guidance on Direct Access; other work took priority.

2.3 Subsequently, the use of Direct Access has now been approved, in PSN terms.

2.4 In terms of devices, current ICT provision was informed by discussions with a group of Councillors about 18 months ago. This concluded that, bearing in mind the Cabinet Office position regarding BYOD and the needs of Councillors then, ICT provision would be limited to a choice of one device from: council provided and managed laptop; council provided and managed tablet; council provided and managed mini-tablet.

2.5 There is a digital revolution under way, however. Never before have changes in technology resulted in such changes in peoples' related desires and expectations, and also there are now many new Councillors, with potentially different needs and wants. It is sensible to re-look at ICT provision therefore.

2.6 As an aside, it should be noted that the PSN also delayed the provision of Wi-Fi in council meeting rooms. In mid-2015 a redesign and rebuild of the Council's network infrastructure now allows a much better Wi-Fi offer to be implemented. For the purposes of this report, therefore, it is assumed that sound Wi-Fi will be available in all council meeting rooms.

3 Scope

4 Councillors' Wants and Needs Explored

4.1 It may be best to explore wants and needs by the use of personas. For example:

A) Councillor A is retired. She spends most of her time either at home, on council business or any of a myriad of other things that one finds to take part in once one has retired. She needs to be able to review reports and emails at home, she does not own a computer herself and so has a council laptop. She maybe would like to read short council emails when she is out and about, but not having this facility has not impacted her life so far. She needs access to reports and other documents during council meetings, but has traditionally relied on paper.

B) Councillor B is working and self-employed. He has limited amounts of time and likes to deal with council business as it arises. Currently he has a council tablet that he can connect to Wi-Fi at home or in the office, but he cannot access emails on the go. He feels frustration at this and believes that it is negatively impacting his contribution as a councillor. He has his own smart phone and 3G/4G enabled tablet for conducting business on the move and would not want other gadgets to carry around. His tablet, if BYOD enabled, would be fine for accessing all he needs during council meetings.

C) Councillor C is working and employed in the education sector. He has limited amounts of time and would like to deal with council business as it arises but his employer does not allow the use of portable electronic devices during school hours. He has a council laptop and fits council business at home around marking and other out of school activities, which he does on a desktop PC. However, at weekends, it would be useful to have access to council emails while on the move. He already has his own smartphone but would be happy to carry a separate council one. He would like to use his council laptop at meetings.

D) Councillor D normally conducts all his business by smartphone. He is used to replying to emails as and when they arise. He can't really see the point in carrying two smartphones, but if the need arose then that's what he would do. He also has an iPad which he brings to council meetings to access the web and public reports, but would also like to access all relevant council documents on it (public and exempt).

4.2   Table 1 attempts to summarise these needs and it is clear that 3 things are required by all: access to emails at home; access to documents at home; access to documents in meetings.

Table 1 - Summary of needs		Councillor			
		A	B	C	D
Access to:					
	Emails at home	✓	✓	✓	✓
	Emails on the move	?	✓	?	✓
Needs	Documents at home	✓	✓	✓	✓
	Documents on the move	✗	✓	✗	✓
	Documents in meetings	✓	✓	✓	✓
Access from:					
	Council device(s) only	✓	✗	✓	✗
	Mixture of council and own devices	✗	✗	?	?
	Own devices only	✗	✓	✗	✓

4.3   The current solution satisfies the common basic needs, assuming that suitable wi-fi provision is accessible in council meeting rooms.

4.4   There are clear differences in how councillors want to conduct council business, however. Some are happy to include it with their work and personal activities, others are happier when there is a clear split between these areas.

5   Bring Your Own Device Policy

5.1   Currently the council does not have a BYOD policy and so any move to BYOD would require such a policy to be put in place, together with training and terms of agreement. There are many various options for BYOD, depending on what aims are most important, and there will be initial costs involved, as outlined in *Appendix B*.

5.2 It should be noted also that any BYOD policy is likely to increase the demands on the ICT Service Desk, especially with queries from councillors around the often blurred edges where personal device support meets business support. Depending on the scale and complexity of those demands, that could add future costs.

5.3 Implementation of a BYOD policy would also attract costs from amendment of the ICT architectural design.

5.4 BYOD does fit with developing the Council's digital strategy and agenda, however. Through this, ultimately is should be possible to make efficiency savings, whilst improving access (and quality) of some services. It is not possible to quantify those savings as yet though.

5.5 The Council has important decisions to take in terms of how ambitious and transformational it wishes to be.

5.6 For example, if it wishes BYOD to simply introduce more choice in access for Members, then in all likelihood the policy would simply cost more.

5.7 If it wishes, ultimately, to *require* Members to use some form of BYOD approach, then that may well change the business case. It may open up many other opportunities and challenges in terms of changing behaviours / transforming how various aspects of council business is conducted – e.g. conducting all meetings in a paperless fashion.

5.8 These sorts of issues will be tested further, as proposals for digital working are developed.

5.9 Any future BYOD policy would need to lay down clearly what information can be accessed from authorised BYOD devices and whether/how that differs from information that can be accessed from council procured and managed devices.

5.10 The policy would have to carefully balance usability and risk.

5.11 These issues are also touched on in *Appendix B*; the Panel's views are sought on these and on the outline options.

6   Data Protection

6.1 The legal responsibility for protecting other people's personal information rests with the data controller, not the device owner.

6.2 The Information Commissioner's Office can impose fines of up to £500,000 for serious data breaches.

6.3 Generally speaking, for council business the Council is the data controller, rather than any individual Councillor.

6.4 Councillors are registered individually as data controllers, however, because in their role they can receive personal information directly from individuals, rather than it coming from the Council. The Council is not the data controller, therefore, in such a situation.

6.5 In light of the above points, there would need to be some consideration of commercial or second party agreements and how these may be affected by BYOD.

7   Risk Management and Security

7.1 For a number of years the Cabinet Office has stated that BYOD should not be considered due to the level of threat posed when using a personal device. Now they have adopted a different stance, which allows local authorities to take a risk based decision on BYOD. The outline options provided in *Appendix B* assume that any solution would be implemented in line with this guidance, recognising and accepting the risks involved.

7.2 Any inappropriate release of information as a result of BYOD, be it personal, confidential or commercial, may seriously impact on the reputation of the Council. It can take years to build a good reputation, but in these times of instant communications it can take seconds to lose it.

7.3 The impact of an information leak can also be high both in financial or operational terms. Historically the chances of such a loss have been low, but this may have been due to tight control by having managed devices separate from councillors' own devices. When using a single device for both council business and personal use there is an increased risk of an information leak, even if technically secure products are used.

7.4 The current threat model for end user devices assumes that devices are fully managed by the organisation, essentially meaning that the devices are an extension of the Council network. If BYOD is to be adopted then this assumption would no longer hold true and there would need to be some changes required to architectural design of the Council's network, to give added safeguards.

7.5 Even if a mobile device management (MDM) solution is used on a personal device, if this MDM solution allows for data to be held on the device then the data could end up anywhere in the world due to automated backups of the device. The level of data encryption and risk of decryption need to be taken into account.

7.6 Authentication to access information on any personal device must be equal to that required to access the information on a Council owned device. This would need to be carefully addressed so that it is not too onerous, otherwise some of the benefits of a single device could be negated.

8   Options

8.1 There are many options available to provide BYOD but in isolation and in simple terms, none would provide a cost saving when compared to the current ICT provision. Net cost savings would only arise if BYOD facilitates other changes in how council business is undertaken. That said, cost-effectiveness may still apply to BYOD, depending on the perceived value attached to the non-financial benefits.

9   The wider Digital context

9.1 As mentioned above there is a digital revolution under way and the exploration /implementation of BYOD is just one small part of a wider issue on how the Council responds to and plans for the associated challenges and opportunities.

9.2 Officers are preparing a report on this for Cabinet early in the new financial year, assuming that the Budget item on Digital Workplace is approved.

10 Conclusion

10.1 BYOD compared to the currently provided technology does not save money initially but it has the ability to significantly enhance the experience for the majority of Councillors. With this improved experience should come greater efficiency and speed of communications, with positive impact on how they undertake their roles, and opportunities to save money. Depending on views therefore, BYOD could offer value for money.

10.2 The choice is basically whether/how far to go with implementing BYOD, and whether it should be used to help with other transformation/digital/ICT developments. This report gives the Panel an opportunity to give its views on these issues.

CONCLUSION OF IMPACT ASSESSMENT
(including Health & Safety, Equality & Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing)
The potential for improved accessibility and communication from BYOD may assist with equality / health and safety to some degree.

LEGAL IMPLICATIONS
Legal Services have been consulted and have no further comments to add.

FINANCIAL IMPLICATIONS
As referred to in the report. It is anticipated that some form of BYOD could be accommodated through the ICT and other budget provisions, as contained in the draft budget to be considered by Council next week.

OTHER RESOURCE IMPLICATIONS
Human Resources/ Information Services / Property/ Open Spaces:
Any key implications are covered in the report.

SECTION 151 OFFICER'S COMMENTS
The s151 Officer has contributed to this report, which is in her name in part (as Chief Officer (Resources)).

MONITORING OFFICER'S COMMENTS
The Monitoring Officer has been consulted and has no further comments to add.

BACKGROUND PAPERS	**Contact Officer:** Chris Riley, ICT Manager
ICT Best Practice Guide – *Reasons not to use personal email for work purposes*	**Telephone:** 01524 582106 **E-mail:** cjriley@lancaster.gov.uk **Ref:**

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.

Budget and Performance Panel 23 February 2016
Bring Your Own Device – High Level Options Analysis

Issues to Consider

Note that there are various other options or solutions, depending on the main aims of any BYOD policy. For example:

− Should BYOD apply to just mobile devices (e.g. smart phones and tablets), or to home computers (PCs)?

− What is the perceived primary purpose of introducing BYOD? Convenience? Improving accessibility and communication? Saving money? Helping to transform how we do business, e.g. having paperless meetings? Something else?

− IF BYOD was introduced in some form, should the Council continue to provide devices at all? In essence, should BYOD be optional, or become a requirement at some point?

Options

1. **Stay with current provision.** This appears to satisfy many councillors' basic needs but clearly with changes in technology and the user/customer expectations that go with these changes, this position is not considered sustainable for long. It may well hinder other future digital developments. There is also the option of providing Members with additional devices to ensure they have adequate connectivity both when on the move or when at home, but this has been discounted.

2. **Have a BYOD policy that allows councillors to use their own smart phones and/or tablets for council business**. This has the advantage that it allows councillors to only have to carry a single device, with access to emails and documents, when working on the move. It would satisfy more needs of councillors but restricts personal choice for BYOD to smart phones and tablets. Changes will be required to the current mobile device management solution. There is a small annual charge per device per year.

3. **Have a BYOD policy that allows councillors to use their own smart phones and/or tablets and/or PCs/laptops for council business**. This has the same implications as 2 above, but in addition, to allow for the use of councillors' own PCs/laptops, it would require implementing a "thin client solution" more appropriately carried out across the Council, which tends to be how other local authorities have implemented it. Here Microsoft Direct Access has been implemented using licences already included in the Microsoft agreement, so the thin client technology would be an addition at significant cost.

4. **Have a BYOD policy that allows councillors to use their own smart phones and/or tablets and or PCs/laptops for council business, using Microsoft Office 365.** This is a cloud based solution that gives the type of business consumer experience that many people expect nowadays. Adopting this option would fit in with other Microsoft software across the organisation. This could act as a pilot for whole organisation move to Office365, which is likely to provide significant savings as a result of escalating on premise costs for Microsoft licences. It would also allow the organisation to start a move towards cloud computing in line with central Government aims.

Indicative Costings

1.1 Assumptions: ICT architectural re-design for BYOD, £6,000; 33% of councillors would adopt some form of restricted BYOD and 66% of councillors would adopt (almost) unrestricted BYOD.

1.2 The way forward could also have a significant bearing on timescales for ICT resources and skills generally. This would need to be addressed (and is not costed).

1.3 If BYOD was adopted as a requirement at some point, this would change the costings. Costs may also be affected by future reviews of the Members' Allowance Scheme (and how/to what extent Members are reimbursed for ICT).

1.4 There are other, potentially more significant financial implications and potential savings linked to changing how the Council does business / how Members undertake their roles.

1.5 In very simple terms though, the direct additional net costs associated with BYOD (over and above current provision) are broadly estimated as follows.

Table Additional Net Cost Comparisons (Indicative) over 4 years

	Option 1 £000	Option 2 £000	Option 3 £000	Option 4 £000
Device savings	0	-11	-11	-22
Redesign costs	0	6	6	6
Set up costs	0	15	45	15
Annual costs	0	3	20	13
Total Net Costs	**0**	**13**	**60**	**12**