DEMOCRATIC SERVICES COMMITTEE – 21ST SEPTEMBER 2016

SUBJECT: BRING YOUR OWN DEVICE FOR MEMBERS

REPORT BY: ACTING HEAD OF INFORMATION TECHNOLOGY

1. PURPOSE OF REPORT

1.1 The purpose of the report is to present the Democratic Services Committee with options and associated information regarding the pre-requisites needed to enable Members to use their personal computing devices to access the Council's information and make recommendations regarding how to progress.

2. SUMMARY

2.1 This report will formalise the pre-requisites that will enable Members to use their personal devices for Council work. It defines the technology and references appropriate legislation and industry standard practices that would underpin a safe and reliable solution.

2.2 The solution has been sized based on each Member being able to register two devices each, such as a smartphone and a tablet.

2.3 Potential options are detailed and the further work required to progress.

3. LINKS TO STRATEGY

3.1 The Local Government (Wales) Measure 2011 requires the Council to provide appropriate support to Members and for the Democratic Services Committee to monitor that support.

3.2 The report links to current strategies employed within the Council to ensure the security and governance of information processed and retained.

4. THE REPORT

4.1 The ability to use personal devices to access the Council's information is generally known as "Bring Your Own Device (BYOD)". There are two main topics that will be covered in this report, namely the technology and the management of information.

4.2 This report will provide advice regarding Members using "true" BYOD at Penallta House on the Ground and First Floors only. This constraint has been applied to limit the scope of the proposal so estimated costs and support calculations could be defined. If necessary the solution can be expanded but this will require further technical investment and incur additional costs which would be identified once any supplementary scope is known. The report also offers less costly options that are not constrained to these areas of Penallta House that may be sufficient to meet Members' access needs.

4.3 Suppliers constrain their BYOD technical solutions to support only the most popular devices used. A “true” BYOD deployment would be constrained therefore by such external influences. However, it is anticipated that the market would ensure that these supported devices and operating systems would be updated to match the changing technical environment over time. It should be noted that additional investment may be required to accommodate such changes in the longer term.

4.4 This report also outlines the environment influences that need to be taken into account when considering such implementations. Such influences will include requirements of the external environment, asset management, information governance and IT security. Key elements related to these categories are included in the following sections.

5. PUBLIC SERVICES NETWORK (PSN)

5.1 The Public Services Network (PSN) is a Government supplied network that facilitates secure transfer of information between the Council and other Public Sector organisations and Government approved service providers. To ensure security of information and the protection of the recipient organisations the PSN enforces annual compliancy assessments. This is a rigorous process with strict rules with non-compliancy resulting in loss of access to the PSN and to the services provided across it.

5.2 There are a growing number of important front line services accessed by the Council that are only available over the PSN and therefore maintenance of compliant status is critical. Examples of such services are given below.

5.2.1 The Department of Works and Pensions (DWP) Customer Information Services (CIS).

5.2.2 The Individual Electoral Registration Database (IER).

5.2.3 The Youth Offending Service central database.

5.2.4 The Blue Badge (Disabled Persons’ Parking) Scheme system.

5.2.5 The Registrars Tell Us Once (TUO) system.

5.2.6 GCSX secure email system operates over the PSN.

5.2.7 LOCTA Search tracing and recovery solution.

5.3 Members’ attention is drawn to the importance of PSN as it enforces strict rules regarding the connection of personal devices. As the Council’s network connects to the PSN these rules need to be applied to the Council’s network. A summary of requirements and other good information governance practices are shown below.

5.3.1 Connection of personal devices will be allowed only where a secure connection is made between the device and the network; ensuring effective user authentication and encryption of information whilst in transit between device and Council’s network.

5.3.2 To reduce the leaking of information the personal device should always be locked when not in use which will reduce the risk of information leakage through “reading over a shoulder” or unauthorised access.

5.3.3 It is preferential not to store business data on the device and it should be saved in protected network locations such as the Council’s data centre. Where data is stored on personal devices it is likely that the device will have both private and business related information on the same device. In these instances a Mobile Device Management (MDM) solution must be implemented to ensure segregation of data on the personal device to enhance the protection of business information.

5.3.4 Some applications installed by the user can automatically share data held on or accessed by the device, e.g. social networking applications may share contacts or calendar information, cloud storage applications may share files as part of a synchronisation process, etc. Such applications must be managed appropriately to minimise risks of sharing business information inappropriately causing information governance breaches.

5.3.5 Where a personal device has been subjected to a virus or other malware attack the perpetrator may gain access to both user and business information inappropriately. As this is the case anti-malware provision and authentication controls to the Council's network must be robust and follow IT security good practices.

6. DEVICE MANAGEMENT

6.1 Management of the device is essential to protect the information accessed and to ensure the security of the network. It is a requirement of the PSN that all devices not supplied and configured by the Council are managed appropriately and specialised MDM software is required to do this.

6.2 MDM is an essential tool to integrate with existing systems, provide the required security measures to allow connection to private wireless networks and help Members meet their obligations as Data Controllers.

6.3 MDM solutions install a small piece of software on the device to facilitate central management of the device and offer the following facilities.

6.3.1 Security Management: Configure stringent security measures to protect business data from outside threats.

6.3.2 Email Management: Segregate business and personal emails on the device so business content may be managed by the MDM solution.

6.3.3 Document management: Provide a secure area on the device to temporarily store business documents providing segregation and encryption of business and personal information.

6.3.4 Application Management: It is possible to manage the applications held on a device remotely preventing download of inappropriate applications or those that present a malware risk. The MDM can also be used to push appropriate Council applications to the device.

6.3.5 In the event that the device is lost or stolen the MDM solution will allow the device to have its data erased helping to protect Members against loss of data and potential infringement of the Data Protection Act.

6.3.6 Asset Management: Capability to scan and retrieve the details of the devices and software installed including the security status of the device.

6.3.7 Device Enrolment: Devices must be enrolled to ensure the specific device is recognised as authorised to access BYOD facilities. Each device that is required to access the BYOD solution must be enrolled separately.

6.3.8 Audit and Reports: Provision of information to be used to minimise information risk.

7. NETWORK CONNECTION

7.1 Personal devices cannot be allowed to connect directly to the Council's network and therefore a separate network with special security facilities is required to act as an intermediary enabling the required access. This combined with an MDM solution will maintain compliance with the relevant PSN requirements.

7.2 To connect a personal device to the Council's network the following must be in place.

7.2.1 The device must be fully up to date with all relevant software. This will include the operating system and all applications installed to ensure all security features and fixes are in place. This will be the device owner's responsibility.

7.2.2 The device must have protection software installed offering defence against virus, other malware and cyber attack that is updated at least daily to reduce the risk of infecting the Council's network. This will be the device owner's responsibility.

7.2.3 The user log-in authentication process for BYOD cannot follow the simple username and password combination deployed within the Council's networks to mitigate security risks. "Two factor authentication" will be required where the usual username and password combination is supplemented by the input of an additional piece of information that only that user knows. The Council currently uses small keyring token devices that display a random number sequence that needs to be input each time a request for access is made.

7.2.4 The device must be enrolled onto the BYOD system to allow access. As devices are replaced the solution will need to be updated with the new device's information as access will be denied from an "unknown" device.

7.3 Specialised networking equipment is required to enable data to be transmitted securely across any non-secured public networks such as the internet. This reduces the risk associated with the data being "inspected" in transit which would enable a cyber attack to be initiated against the Council.

8. DATA PROTECTION ACT

8.1 In the event of a Subject Access Request or Freedom of Information Request there is a risk that data backed up by users may no longer be under the control of the Council and may come to light at a later date. This could place the organisation at risk of reputational damage and legal or regulatory non-compliance and the Council's already comprehensive Members' information governance training programme would need to be supplemented to cover such eventualities.

9. EQUALITIES IMPLICATIONS

9.1 This report is for information purposes, so the Councils EqIA process does not need to be applied.

10. FINANCIAL IMPLICATIONS

10.1 The solution on which the cost estimates have been based would be open to all Members and their IT support staff and offer a maximum of two devices per user, e.g. a smartphone and a tablet. This equates initially to approximately 160 devices.

10.2 "True" BYOD - The following costs are cost estimates for a "true" BYOD implementation but would need to be confirmed once the final requirements and solution have been established.

Item	Unit Cost	Quantity	Total	
Specialised Network Equipment	£4,000	1	£4,000	
Associated Licences	£40	160	£6,400	
Associated Maintenance	£560.00	1	£560	per annum
MDM Server Equipment	£2,400	1	£2,400	
Associated Licences	£90	160	£14,400	per annum
Associated Maintenance	£336	1	£336	per annum
Two Factor Authentication	£90	77	£6,930	3 year cost
Training & Installation	£550	1	£550	
Implementation & Configuration Professional Services	£1,200	4	£4,800	
IT Implementation & Initial Support Costs			£18,800	6 months' cost of Grade 8
IT On-Going Support Costs			£11,300	30% of Grade 8 p.a.
Year 1 Costs			**£70,476**	
Year 2 Onwards Costs			**£26,596**	per annum

10.3 Alternative Options - Other options are available dependent upon the service requirements. The following alternatives have been identified as lower cost options that will deliver access to email and calendar facilities from non-Council devices and therefore may deliver some of the desired benefits.

10.3.1 Outlook Web Access. Email and calendar services could be made available for supported tablet devices with no additional costs. It should be noted that resources from the IT Department would need to be deployed to configure and support the service and be scheduled into its work plan.

10.3.2 Outlook Mobile Access. Email and calendar services could be made available for supported smartphone devices with the additional costs outlined below. It should be noted that resources from the IT Department would need to be deployed to configure and support the service and be scheduled into its work plan.

Item	Unit Cost	Quantity	Total	
Additional Device Licences	£55	77	£4,235	
MDM Server Equipment	£2,400	1	£2,400	
Associated Licences	£90	80	£7,200	per annum
Associated Maintenance	£336	1	£336	per annum
IT Implementation & Initial Support Costs			£6,300	2 months' cost of Grade 8
IT On-Going Support Costs			£7,500	20% of Grade 8 p.a.
Year 1 Costs			**£27,971**	
Year 2 Onwards Costs			**£15,036**	per annum

10.4 Funding sources would need to be identified as part of any resultant business case process.

11. PERSONNEL IMPLICATIONS

11.1 The solution will be open to all Members and their IT support staff and initially 160 devices, there will be a need to support these devices. In addition to the device support there will be considerable support required for the management and support of a "true" BYOD solution and a lesser requirement for other options. This could be absorbed into the work of the existing workforce but would have an impact on the capacity to undertake other work, e.g. prioritisation of activity may lead to greater time required to implement changes / support solutions. These opportunity costs have been incorporated into the Financial Implications section of this report.

11.2 There would be a training requirement for Members for accessing the BYOD solution and identifying risks associated with use of this solution.

12. CONSULTATIONS

12.1 There are no consultations that have not been included in the report.

13. RECOMMENDATIONS

13.1 It is recommended that a project team is created to produce a detailed specification of requirement for Members' access to IT solutions. It is suggested that this team be made up of a representative from each political group and key Democratic Services and IT members of staff.

13.2 That this group also considers the IT device and service requirements for Members for the period following the local elections in May 2017.

14. REASONS FOR THE RECOMMENDATIONS

14.1 The costs associated with BYOD can be significant. A definitive specification of requirements is required so that service implications and costs can be derived to inform any business case to implement changes.

14.2 Members' IT provision was subjected to a holistic review at the time of the last local elections. This review had a positive impact informing the service and devices offered. The technologies now available have developed since that time and their adoption may facilitate the service provided for the next post-electoral period.

15. STATUTORY POWER

15.1 This report has been prepared following the Statutory Guidance relating to the Local Government (Wales) Measure 2011; Chapter 3 Section 16: Democratic Services Committee.

Author: Paul Lewis – Acting Head of IT and Central Services
Consultees: Nicole Scammell – Acting Director of Corporate Services
Gail Williams – Interim Head of Legal Services & Monitoring Officer
Catherine Forbes-Thompson – Interim Head of Democratic Services
Gwyn Williams – Acting ICT Operations Manager
Alessandra Veronese – E-Government Team Leader
Joanne Jones – Corporate Information Governance Manager