WARWICK DISTRICT COUNCIL

INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Remote Working and Portable Devices Audit
TO:	Head of Corporate & Community Services		
C.C.	ICT Services Manager ICT Applications Support Manager	**DATE:**	27 February 2013

1 INTRODUCTION

1.1. In accordance with the Audit Plan for 2012/13, an examination of the above subject area has been completed recently and this report is intended to present the findings and conclusions for information and action where appropriate.

1.2. Wherever possible, results obtained have been discussed with the staff involved in the various procedures examined and their views are incorporated, where appropriate, in any recommendations made. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 SCOPE AND OBJECTIVES OF AUDIT

2.1 The Council's requirements with regard to remote working are stated within two separate policies. These are the Remote Working Policy, which covers employees and councillors, and the ICT Services – Third Party Network Access Policy, which covers suppliers, contractors and partners. The audit focused upon the key controls in place around the approval, allocation and security of portable devices and remote working facilities.

2.2 The evaluation was based on the following control objectives:

- A strategy for the use of remote access and portable devices is in place and has been formally approved as part of the overall ICT strategy;
- Value for money is supported through a defined strategy on portable device selection;
- Responsibilities for risk assessment, acquisition, configuration, distribution and management of remote access facilities and mobile devices are formally assigned;
- Risks relating to the use of remote access and mobile devices have been formally assessed against the objectives that supported their introduction and a risk management approach has been specified for each identified risk.
- Access to ICT services and data resources is adequately controlled;
- Appropriate procedures are in place with regard to the transfer of data from and to portable devices;
- Effective use of devices and remote access is supported by training, guidance and support.

2.3 The audit approach aimed to assess the approach towards remote access and portable devices through:

- examination of documentary evidence in respect of strategies, policies, risk assessments, assignment of responsibilities, and operational procedures; and
- consultation and discussion with key officers associated with the provision, management and monitoring of remote access and portable devices.

3 FINDINGS

3.1 Strategy for Remote Access and Portable Devices and Value for Money

3.1.1 TheICT Strategy states that technology's role is to support staff when they adopt agile working methods. This is primarily about giving staff access to their IT systems, data and telephony via an appropriate device e.g. desktop PC, laptop, smartphone or VOIP handset. The desktop strategy of the Council is to make access to Council systems device and location agnostic. All service provision is subject to an effective risk assessment process that allows informed business decisions and security measures to address the need for confidentiality, integrity and availability of information.

3.1.2 Value for money is considered within every strategic decision made by ICT. For example, the recent report to SMT on the Use of Personal Devices to access Council Email addressed both the benefits and the impact on budgets of implementing the Good Technology software. Value for money with regard to laptop machines and tablets is ensured by the ICT team. A list of suppliers is maintained and assessment made based on the required criteria each time a purchase is to be made. The provision of mobile phones was reviewed in 2012. For smartphone devices and data charges, a consultant was brought in to provide a value for money assessment. This resulted in the introduction of new contracts and centralised procedures.

3.2 Responsibilities Relating to Remote Access Facilities and Mobile Devices

3.2.1 The ICT team takes responsibility for all aspects of remote access provision. This includes provision and management of the remote access mechanisms and the implementation of controls to protect data at rest on the devices themselves. This is in line with the Remote Working Policy. Laptops and tablets are purchased via ICT. Contracts relating to mobile phones and data charges are managed outside of ICT by the responsible officer within Housing.

3.3 Risk Assessment

3.3.1 The risks relating to the provision of remote access and the mobile devices can be simplified into three key risks. These are:

- Unauthorised real-time access to *centrally held services and data* from outside the network, thus leading to disclosure of data.

§ Unauthorised access to *data stored on portable devices,* leading to disclosure or loss of data. This can include laptops, tablets and smartphones; and

§ Unauthorised access to *data stored on portable media* that has been written from the network, thus leading to disclosure of data.

3.3.2 The primary objective for remote access and mobile computing at WDC relates to agile working. An effective risk assessment should be structured around the concept of outcomes against this objective, with the identification of each outcome allowing threats and impacts to be identified. In turn, these allow gross risks and residual risks to be calculated.

A formal risk assessment has been undertaken and documented by the ICT team in the form of the 'Risk Assessment for Remote Access'. The assessment considers aspects of thethree primary risk outcomes as shown in 3.3.1 above. It also covers some of the underlying threats that apply via current remote mechanisms and portable devices/media. This is felt to be adequate in relation to this audit. Internal Audit have provided an advice note to ICT on how the assessment could be further developed if required.

3.4 Control of Access to Resources and Controls Over the Transfer of Data

3.4.1 Five methods are in place that allow remote access to networked resources. All methods require Active Directory authentication plus – with the exception of Outlook Web - one or more other factor. The methods are as follows:

§ Cisco IPSEC VPN 1 with RSA token;

§ Cisco AnyConnect SSL VPN without RSA token;

§ VMView thin client desktop with RSA token;

§ Outlook Web email access via the internet;

§ Smartphone access to email via Microsoft Active Sync plus the use of Good Technology for use with members' own devices.

Each method is specified for use by one or more target group of users. The Cisco AnyConnect SSL VPN method is used for third party vendor access. Whilst this does not include RSA authentication, procedures provide for vendor Active Directory accounts to be disabled by default and to only be enabled when remote support is to be provided.

The methods in place are well understood and utilised by ICT to support the objective of agile working. A small number of issues were identified, however. These are shown at 3.4.2 – 3.4.4 below.

3.4.2 Staff who access the internet via their remote access connection should do so through their VMView thin client desktop. This routes internet access via the Council's internet service provider and so is subject to web filtering and controls. Whilst laptop settings should ideally prevent users bypassing these controls, issues with VMView led to this beingpermitted pending identification and implementation of a solution.

Risk
Inappropriate material could be accessed via Council laptops.

Recommendation
Potential mechanisms for preventing uncontrolled access to the internet from Council-issued laptops and tablets should be investigated with a view to implementation. It is understood that the favoured solution is the application of filtering in the cloud via Sophos Mobile Device Management. Other possible solutions could include an upgrade to the VMView client to enable browser settings to be successfully locked down.

3.4.3 Remote access to networked resources is provided via five different mechanisms, as shown under 3.4.1.The provision of remote access provides an increased risk of unauthorised access and a combination of preventative and monitoring measure should therefore ideally be applied. Whist some logging of events is undertaken, the data is only utilised for investigating reported issues.

Risk
Inability to proactively identify and address attempts to gain unauthorised access via named login accounts.

Recommendation
The potential for monitoring failed log on attempts and locked accounts should be investigated with a view to identifying key security events that could indicate unauthorised access attempts; ensuring that such events are actively logged; specifying criteria for the most significant security events i.e. those that require investigation; and introducing reporting and investigation processes for the most significant events.

3.4.4 The Active Sync product is provided with Exchange Server 2010 and allows ICT to provide policy-based controls over mobile device connections to Council email. The configuration options are user-based and therefore permit ICT to allow or deny access to individual users via a mobile device and to provide policy-based controls over the device. Active Sync does not control which devices a user is able to connect, however; so long as the user is enabled and the device is provisionable (i.e. is compatible with Active Sync), then a user is able to connect multiple devices.

The Council policy on mobile connections is to only allow Council-owned devices to be connected by staff. This can only be enforced by reporting all devices that have connected and then identifying any that are not Council-owned. Whilst an initial exercise was undertaken when the policy was introduced, ongoing checks are not in place.

Risk
Non-adherence to Council Policy and that disclosure of data could occur in the event of an unauthorised mobile device being lost or stolen.

Recommendation
Periodic monitoring of devices connected via Active Sync for synchronised downloads should be introduced to identify:

- Any devices that are registered to staff via Active Sync but which are not Council-issued;
- Any devices that are registered to members via Active Sync and which have not had Good Technology installed and configured.

Any unauthorised devices that are identified should be referred to the line manager or to an appropriate senior manager where the issue relates to members.

It is understood that the Sophos Mobile Device Management (MDM) module is to be purchased shortly. The potential for implementing these checks via MDM should be investigated with a view to simplifying and automating this monitoring as far as possible.

3.4.7 The transfer of email to local storage on mobile devices is managed via the Active Sync product, which is provided with Microsoft Exchange server. This provides for email to be synchronised to the devices.Staff with Council-owned smartphone devices are permitted to access email, together with members who are permitted to access via their own devices. The Good Technology product is currently being implemented for members to provide additional security over personal devices. This will also support the process of synchronisation.

3.5 **Training, Guidance and Support**

3.5.1 Written guidance as to the responsibilities of users is provided in the Remote Working Policy. The document also provides extensive guidance on the security procedures to be applied when remotely accessing networked resources and when using portable devices off-line. One to one guidance is provided by the help desk when remote access is assigned to a user and help can be gained from the Help Desk on demand.

3.5.2 A contract is in place with an external support company that allows WDC ICT to submit any security concerns and questions. The company concerned also run periodic penetration tests for WDC and this specifically addressed remote access mechanisms for the test in late 2012.

4. CONCLUSIONS

4.1 The provision of remote access to networked resources and the use of Council-issued and personal portable devices to access these resourcesis designed to address the need for agile working. The ICT team take a proactive and risk-based approach to supporting this requirement.

4.2 A number of issues have been raised in the report. All are rated as medium priority.

4.5 In view of the above issues, the findings are considered as giving SUBSTANTIAL assurance that appropriate controls are in place to effectively manage the risks relating to remote access and the use of portable devices.

6. MANAGEMENT ACTION

6.1 Recommendations to address the issues raised are reproduced in the appended Action Plan for management response.

Richard Barr
Audit and Risk Manager