Leeds
CITY COUNCIL

Originators: Andy Nutting
Tel: 07545 604251

Report of the Assistant Chief Executive (Policy, Planning and Improvement)

Corporate Governance and Audit Committee

Date: 14th December 2010

Subject: Security Arrangements for PDA Devices

Electoral Wards Affected:

□ Ward Members consulted (referred to in report)

Specific Implications For:

Equality and Diversity □

Community Cohesion □

Narrowing the Gap □

Executive Summary

Breaches of information security and losses of data, both nationally and at a local level, have focused public authorities to become more accountable for security failures or for the contravention of procedures which lead to the loss or disclosure of sensitive information.

Leeds City Council has recognised the need to protect its information assets from both accidental and malicious loss or damage. Information security is taken very seriously by the Council and this is evidenced by the ongoing work to improve the security of its information.

This report focuses on the technical security arrangements that have been put in place for PDA (Personal Digital Assistant) devices issued by the Council; but also highlights work being undertaken to introduce supporting policy and procedures relating to people and process. This report aims to provide assurances that information contained on PDA devices is secure should the user of such a device lose it or have it stolen.

1.0 Purpose Of This Report

1.1 After considering a report about information security on 29th September 2010, Members of the Corporate Governance and Audit Committee requested a further report detailing the security arrangements the Council has in place for PDA devices issued by the Council. The content of this report provides Members of the Committee with this information.

2.0 Background Information

2.1 Leeds City Council has recognised the need to protect its information assets from both accidental and malicious loss or damage. Information security is taken very seriously by the Council and this is evidenced by the ongoing work to improve the security of our information as outlined in this report.

2.2 This report provides Members of the Committee with details and assurances about the security arrangements in place for PDA devices issued by the Council.

3.0 Main Issues

3.1 Personal Digital Assistants (PDA's) are approved at a departmental level and are only issued by ICT services on receipt of a valid finance code and payroll number (so we know who has the device). The Council has an approved contract with preferred supplier Damovo for the supply of PDA's. The network services are in turn provided by O2. There are approximately 800 devices currently in use across the Council, all of which are based on the Microsoft Windows Mobile Operating System.

3.2 PDA's pose a potential security risk to the Council in that due to their small size they are easy to lose, however large amounts of information can be stored on them. The Council recognises the business benefits such devices bring, but also recognises the need to mitigate against the loss or theft of such devices. The Council has implemented security protection both from a technical and policy (people and process) perspective and this report highlights the work undertaken to this extent.

3.3 Information is transmitted to and from PDA devices from a dedicated O2 Access Point Name (APN) located on the Council's network. This means that information between the Council network and the PDA device remains encrypted across the mobile network and cannot be intercepted.

3.4 Information held on the PDA is encrypted using the Microsoft encryption inherent in Microsoft Exchange 2007, and since the device has to attach to the Microsoft Exchange system in order to synchronise the Microsoft Outlook functions of email, calendar, contacts and notes - the encryption policy can be enforced. This encryption also extends to any removable memory cards (MicroSD) rendering these unreadable from other devices. There are also additional controls available within the Microsoft 2010 suite of products (and other products) and these are currently being evaluated for the future. This may well enable personal PDA devices (non-Council) to be rendered sufficiently safe to use at some point. Other Local Authorities are already using personal PDA's to access Council e-mail services etc.

3.5 Security arrangements for the PDA's are further enhanced as Corporate ICT Services are able to remove information from any device lost or stolen - even with the device in 'stand-by' mode. Furthermore, if a PDA is lost or stolen, it can be permanently disabled. This will occur after the device has been effectively wiped of its MS Outlook based data. All device numbers are recorded centrally and are used to inform Damovo who are able to disable the device and render it unworkable. This can only be done if the loss or theft is reported and it is critical that Corporate ICT Services are informed of all such incidents so that they can take the appropriate remedial action. It is the responsibility of users to inform the Corporate ICT Helpline if a device is lost or has been stolen so that it can be disabled.To this extent, a process for reporting such incidents is being established as part of the Information Incident Management policy. To put this all into perspective, there have been six devices disabled in the last 6 months either because they were stolen or mislaid. In two instances, the devices were subsequently recovered.

3.6 When issued to users, all PDA devices are supplied with a PIN lock, which is a four digit code unique to each device. This four digit PIN is selected by the user on first receipt of the PDA and is used to unlock the device prior to repeated use. This is done in the presence of the ICT onsite support team and forms part of the configuration process. Furthermore, should the PIN be entered incorrectly eight times, the PDA will lock and it will need to be returned to Corporate ICT Services to be rebuilt. The ICT onsite support team will also issue general guidance on the sensible use of the device e.g. choosing a sensible and safe PIN number.

3.7 PDA devices can access internet services, but access is filtered to reduce the likelihood of people accessing inappropriate sites. If required, internet usage can be monitored at the device level, however, the Council does not monitor the usage of such devices or monitor connections as a matter of course.

3.8 Whilst the technical arrangements put in place to protect and secure the information stored to PDA's are necessary, these need to be backed up by appropriate policy and supported with relevant processes and guidance. To this extent, the following policies are in various stages of development and will support the security arrangements put in place for PDA devices:

- Removable Media and Mobile Computing - establishes the principles and working practices that are to be adopted by all users in order for information to be safely stored and transferred on removable media - including laptops and PDA's. This policy is drafted and is on the final round of consultation within the Council and will be approved by 30th November 2010;

- Acceptable Use Policy - protect all information assets owned and used by the Council from the risks posed by inappropriate use, including virus attacks, compromise to network security and services, disclosure of information as well as legal and regulatory issues. Furthermore, this policy will be supported by a number of guidance notes, one of which will include instruction notes to PDA users about how to change PIN's, use sensible PIN number combinations and keep the device physically secure. This policy is drafted and is currently going through consultation with officers and the trades unions. It will be approved by 31st March 2011;

- Information Incident Management Policy - to ensure that the Council reacts appropriately to any actual or suspected security incidents relating to information systems and information. This will be supported by a corporate procedure to report the loss or theft of information or equipment storing information. This policy is drafted and is currently going through consultation with officers and will be approved by 31st January 2011.

3.9 The development of these policies forms part of the Information Governance Project. The aim of the Information Governance project is to ensure all Information Governance policies are developed and embedded across the Council through an effective communications, engagement and training plan. Corporate ICT Services are contributing to the development of these policies in order to ensure that they support the implementation of security systems and related technologies. All policies are being developed as part of the Council's Information Governance Framework and as such will be signed-off by the Assistant Chief Executive (Planning, Policy & Improvement) under a Delegated Decision Notice.

3.10 Discussions with the Members' Development Officer are taking place in December 2010 about identifying the most affective and appropriate way of ensuring Members are involved with the consultation process for the information governance polices that are likely to have an impact on them.

4.0 Implications For Council Policy And Governance

4.1 The technical arrangements for securing PDA devices needs to be supported by relevant information governance policies which effect people, process and decision making. These policies are outlined in paragraph 3.7 of this report and form part of a series of policies developed for the Information Security module of the Information Governance Framework. The Information Governance Framework was approved by the Executive Board in November 2008.

4.2 All Information Governance policies and procedures will follow a consultation process to obtain support and approval and this includes the Council's Information Governance Management Board (IGMB), Resources and Performance Board and the Corporate Governance Board.

5.0 Legal And Resource Implications

5.1 Sufficient capacity is identified within Directorates to be able to act and respond to an information security incident and to follow the procedures outlined in the Information Incident Management Policy.

5.2 In order for the Council to comply with its obligations under the Data Protection Act, it must deploy technologies, processes and guidance to ensure the security of personal information. The developments that have already taken place and the actions that are currently being undertaken will ensure the Council identifies and mitigates against current and emerging threats and helps prevent security breaches occurring.

6.0 Conclusions

6.1 Mobile devices pose a potential risk to the security of the Council's information. This report outlines the measures being undertaken by the Council to improve security to removable media, and specifically PDA devices, in respect of technical deployment and policy (people and process) implementation.

6.2 Corporate ICT Services have put into place the necessary technical arrangements for securing information held on PDA devices by deploying encryption and pin lock codes to PDA devices and ensuring there is a mechanism in place to disable devices should it become necessary. These measures are complemented by the implementation of policies aimed at embedding the processes and guidance across the Council required to improve our information security; such as the reporting of information security incidents and the acceptable use of information and ICT.

7.0 Recommendations

7.1 Corporate Governance and Audit Committee are asked to consider the contents of this report and the assurances provided about the security arrangements in place for PDA devices issued by the Council.

Background Documents Used

Information obtained from Corporate ICT Services

Draft Information Incident Reporting Policy

Draft Removable Media and Mobile Computing Policy

Draft Acceptable Use Policy