

# Dacorum Borough Council – Final Internal Audit Report

## Information Security

### Distribution list:

Sally Marshall – Director of Finance and Corporate Services

Chris Gordon – Group Manager Performance, Policy and Projects

### Key dates:

Date of fieldwork: September/November 2011

Date of draft report: December 2011

Receipt of responses: January 2012

Date of final report: January 2012

This report has been prepared on the basis of the limitations set out in Appendix C.

This report and the work connected therewith are subject to the Terms and Conditions of the Contract between Dacorum Borough Council and Deloitte & Touche Public Sector Internal Audit Limited. The report is produced solely for the use of Dacorum Borough Council. Its contents should not be quoted or referred to in whole or in part without our prior written consent except as required by law. Deloitte & Touche Public Sector Internal Audit Limited will accept no responsibility to any third party, as the report has not been prepared, and is not intended for any other purpose.

# Contents

- 1. EXECUTIVE SUMMARY 3
- 2. SCOPE OF ASSIGNMENT 6
- 3. ASSESSMENT OF CONTROL ENVIRONMENT 8
- 4. OBSERVATIONS AND RECOMMENDATIONS 9
- APPENDIX A – REPORTING DEFINITIONS 34
- APPENDIX B – STAFF INTERVIEWED 36
- APPENDIX C - STATEMENT OF RESPONSIBILITY 37

# 1. Executive summary

## 1.1. Background

This audit forms part of the agreed 2011/12 Internal Audit Plan with Dacorum Borough Council.

A number of high profile data security breaches have been recently reported within the media and have focused Government organisations on the need to have strong processes in place to protect their data which may be confidential or sensitive. These events, along with a number of reports into Government data handling and transit, have raised awareness and highlighted the need for organisations to review their existing information security arrangements to help ensure that robust security policies and practices are in place.

Furthermore, recent changes in legislation have enabled the Information Commissioner to issue strong warnings over the consequences of data losses including the ability to impose substantial penalties over any breach or loss. As a result, the Public Sector have identified the requirement for organisations to have strong Information Governance and Information Security controls in place to protect data held by the organisation and to assist in the compliance with the Data Protection Act 1998.

As a result of a break in at the Bennetts End Adventure Playground in August 2011, the Council requested internal audit to undertake audit work around the Council's usage of Information and identify the controls in place to identify, collect, manage and dispose of sensitive or personal information that the Council holds.

Information Security is the practices and policies that an organisation has in place to safeguard information assets and includes both technical controls over IT assets and electronic data and awareness and procedural controls over the use and management of information assets.

## 1.2. Objectives and Scope

The overall objective of this audit was to provide the Members, the Chief Executive and other officers with reasonable, but not absolute, assurance on the adequacy and effectiveness of the key controls relating to the following areas: Network Security, Information Governance and through sample visits to outlying Council offices.

In addition we also undertook a fact finding exercise of the Bennetts End data theft and this is reported separately in the Final Internal Audit Report – Bennetts End Data Theft, November 2011.

## 1.3. Summary assessment

Based on the work undertaken, as detailed in the 'Audit Objective and Scope', we found that Weaknesses in the system of internal control design are such as to put the system objectives at risk.

Our assessment in terms of the design of, and compliance with, the system of internal control covered is set out below.

Evaluation Assessment	Testing Assessment
Limited	Limited

Management should be aware that our internal audit work was performed according to UK Government Internal Audit Standards which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board.

Similarly, the assessment gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board. The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A, whilst further analysis of the control environment for Information Security is shown in Section 3.

#### 1.4. Key findings

We have raised five priority 1 recommendations, fifteen priority 2 recommendations and four priority 3 recommendations, where we believe there is scope for improvement within the control environment.

These are summarised below:

- **IT Security**

Security of the Council's network as well as its data and information is dependent on appropriate IT security controls being defined and policies being implemented. We looked at various areas of IT security as set out in the scope of the audit and found that, although there are controls and policies in place, these should be enhanced to improve security and provide a greater level of protection. For example, we have recommended that the network password controls be improved, greater audit logging and monitoring is performed, additional authentication is introduced for remote access, the requirement to perform a laptop asset audit to help ensure that the latest security controls have been employed on all portable PCs, similarly all mobile phones that have an email and data capability should have additional protection such as passwords and encryption enforced when issued as standard. In addition, we have also recommended that only approved Council issued encrypted USB devices be permitted.

- **Information Security and Governance**

As defined in the audit scope, we performed audit testing on the Information Security Policies, roles and responsibilities over Information, Data Classification and Asset Ownership. As a result of our audit, we identified that currently Information Asset Owners have not been identified for Council information, that there is no process in place to identify and classify data according to its sensitivity. We also identified that there is no formal records management process in place. Our audit identified that although a data sharing protocol is in place, this was created in 2001 and has not been reviewed for some time. In addition, we could not identify who had signed up to the protocol. Although the Council has a number of policies and procedures established for Information Security, these could benefit from consolidation into a single document covering all major areas of IT related security. We also have recommended that the ownership of this document be formally assigned as the Information and data sharing protocols and agreements in place have not been reviewed for a long time to confirm validity and adequacy and since the departure of the Information Security Officer, there is currently no specific designated Security Officer in post. This role is currently performed by an IT officer who apart from this role and their other IT roles is also designated as the Records and Data Management officer.

- **Site Visits**

As a result of the original information security incident, we also visited three randomly selected

sites within the Council – Chaulden Children’s Adventure Playground, Berkhamstead Civic Centre and the Woodwell Cemetery. Some of the issues identified include records created on spreadsheets or databases that are not protected, records are retained longer than necessary, and access to files and folders is not restricted.

Full details of the audit findings and recommendations are shown in Section 4 of the report.

### **1.5. Management Response**

*We have included a summary of the management responses in our Final report.*

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this audit.

## 2. Scope of assignment

### 2.1 Objective

The objective of the internal audit was to identify the controls that the Council has in place over the security of its Information Assets. This looked to provide assurance over the controls that have been established to identify that information and data is held securely and in line with legislative requirements and to help ensure that suitable controls have been established over the management and protection of data from a technology point of view.

### 2.2 Approach and methodology

The following procedures were adopted to identify and assess risks and controls and thus enable us to recommend control improvements:

- Identification of the role and objectives of each area;
- Identification of risks within the systems, and controls in existence to allow the control objectives to be achieved; and
- Evaluation and testing of controls within the systems.

### 2.3 Areas covered

In accordance with our agreed terms of reference, our work was undertaken to cover the following audit areas:

#### **IT Security**

- Security Incident Review – To undertake a fact finding exercise to understand the events that have occurred as part of the data loss at an Adventure Playground. (Reported separately in Final Internal Audit Report – Bennetts End Theft, November 2011.
- Network Security Password Controls and User Authorisation – To help ensure password controls have been established that conform to best practice and effective controls are in place to authorise access permissions.
- Data Management and Corporate File Structure – To undertake system testing to identify how the Council has structured its data on the network and to authorise access to users within the Council.
- Mobile Data Security and Data Management – To undertake testing on the controls the Council have in place over Mobile Devices including Smart Phones and laptops. This will include the process for Security controls over the device. The process for managing data within the device, including encryption, asset management and processes for dealing with loss of the device.
- Use of Portable Memory Devices – To audit the controls in place over the use of portable data devices including USB and CDs.
- Secure use of data transfer – To undertake audit work into the secure use of email data devices, third party email accounts and any other methods of data transfer.

- Data Disposal – To identify methods of data destruction and the process for decommissioning devices used within the Council.

### **Information Security and Governance**







- Information Security Policies – To help ensure formal and up to date security policy and procedures exist to protect the Information Systems infrastructure.
- Information Roles and Responsibilities - To help ensure roles and responsibilities with regard to Information Risk have been established within the Council in line with best practice guidelines.
- Information Classification and Asset Ownership – To assess the processes for information asset identification and classification of information assets. Identify if information assets have been assigned ownership.
- Information Sharing - To identify the processes in place for the identification of sharing of Council information and processes in place to securely share this information.
- Information Security and Governance Training and Awareness – To establish the processes for raising awareness of Information Security.
- Incident Management – To establish the processes for the reporting and management of information security breaches.

### **Dacorum Council site Visits**

As part of this audit work we conducted a series of site visits to Council outlying offices and locations where information is held on Dacorum PCs to identify the processes for managing Council data and information and associated security controls. This included looking at the methods for storing data, password access, IT Physical Security Controls, back up arrangements to provide assurance that data located outside the Civic Centre is subject to IT security controls.

### 3. Assessment of Control Environment

The following table sets out in summary the control objectives we have covered as part of this audit, our assessment of risk based on the adequacy of controls in place, the effectiveness of the controls tested and any resultant recommendations.

<b>Control Objectives Assessed</b>	<b>Design of Controls</b>	<b>Operation of Controls</b>	<b>Recommendations Raised</b>
<i>IT Security</i>			<b>Recommendations 1 - 11</b>
<i>Information Security and Governance</i>			<b>Recommendations 12 - 18</b>
<i>Site Visits</i>			<b>Recommendations 19 - 25</b>

The classifications of our assessment of risk for the design and operation of controls are set out in more detail in Appendix A.



## 4. Observations and Recommendations

### 1. IT Security

#### Recommendation 1: Remote Access Controls

(Priority 1)

##### Recommendation

A review of remote access security controls should be performed with a view to implementing additional security controls for access connections into the Council's network, for example:

- Implementing two-factor authentication controls for remote access to enhance security;
- A policy and process should be established to help ensure that all devices connecting to the Council's network have up to date Anti-Virus and Spyware software in place and that this is regularly updated;
- All PCs accessing remotely should have up to date security patches in place; and
- Restrictions should be established to help ensure that all users are not permitted to download Council data onto PCs unsupported and not owned by the Council.

##### Observation

Additional remote access controls will help to ensure that the confidentiality and integrity of the Council's network and its systems is greatly improved and protected as additional controls improve authentication to Council data and do not permit Council data to be loaded onto unsupported devices.

We identified that in order to remotely connect to the Council's network, the user is required to enter a username and password in the secure website: [ssl.dacorum.gov.uk](https://ssl.dacorum.gov.uk). No further authentication is required and no checks are made on the user's PC to help ensure that their Anti Virus protection is up to date or that it has got the latest security updates and patches applied. We further ascertained that the user is able to download or copy data from the remote network connection to the local drive of the PC.

Without additional remote access security controls, there is a risk of unauthorised access to the Council's network and therefore access to its data. There is the possibility of Council's data being downloaded and available to unauthorised personnel which could be embarrassing to the Council and could constitute a potential breach of the Data Protection Act 1998. There is also the risk of virus or security breaches being introduced into the Council's network through poorly patched PCs and mobile devices.

##### Responsibility

John Worts – ICT Team Leader

##### Management response

###### Agreed

A policy and process review using best practice on all ICT security practices and policies will be completed by the end of March 2012. Role out of the new procedures will also take place to ensure that procedures meet the policy will take place by the end of May 2012.

**Recommendation 2: Review of Access to Drives, Directories and Folders (Priority 2)**

**Recommendation**

Access to network drives, directories and folders should be reviewed and where this is deemed not necessary or required for users’ day to day operations, the access should be removed. Where access is required to other departmental shared drives, directories or folders, the reasons for its access should be provided and approved by the information owner of the relevant Department before the access is approved.

Furthermore, a process should be introduced to periodically review the access granted/available to ensure that it is still valid and required for the purpose required.

**Observation**

The review and restriction of user access to only data that is required for their job roles will help to ensure that users only have access to data and information that they need to fulfil their role and responsibilities.

On a sample of user’s PCs we identified that users have access to network drives, directories and folders that they do not need or have far greater access than needed for the purpose required. For example, we found that:

- In Children’s Services, a user had access to both ‘F’ and ‘Y’ drives which had identical information held on it and the user only needed access to one folder on the ‘F’ drive;
- In Revenues and Benefits, a user had access to the ‘J’ and ‘S’ drives which the user was not sure of the reason as this level of access was not in place; and
- In HR, a user had access to the ‘P’ drive, however the user only needed temporary access to a particular folder in that drive. The user also had access to ‘S’ and ‘X’ drives which he was not sure why and didn’t think he needed that access.

Audit also observed at the Berkhamsted Office that:

- user access was available to the L: drive, which includes a ‘Payroll’ folder, with access to an Excel spreadsheet named: ‘Car Mileage for Aylesbury Vale DC’; and
- The M: drive contained various work-related documents, i.e. daily occupation of halls analysis and protection had not been applied to any spreadsheets to restrict access to information.

Failure to review and minimise access granted on a ‘need to have’ basis, could result in users gaining access to data or information that they are not authorised or entitled to see. This could result in uncontrolled access to information that could be sensitive. There is also a risk that over time access to network drives may not be controlled and this could lead to excessive access to sensitive data directories.

**Responsibility**

John Worts – ICT Team Leader

**Management response**

Agreed Procedures for access to drives and access monitoring will be drawn up to ensure the information owner agrees to access being given before access is granted to individuals.

End of February 2012 completion.

A review of the use of current drives and access to them will take place with changes to access being made subject to the approval by managers.

End of June 2012 completion.

**Recommendation 3: Laptop Management**

**(Priority 1)**

**Recommendation**

An exercise should be undertaken to identify all Council owned laptops and once identified, an inventory record should be created recording all laptop details. The database should include configuration details such as the make and model of the laptop, version of the software, who it is assigned to and the details of the asset numbering.

Once this exercise has been undertaken, the laptops should be reviewed to ensure that they meet the Council’s current security requirements and have hard drive encryption, an up to date and patched operating system and up to date anti-virus software. If the reviewed laptops do not meet the expected standard, they should either be upgraded to the required specification or removed from use.

Additionally, we recommend that all new laptops issued are accompanied by relevant guidance to users such as, the Council’s policy on the use and security of laptops.

We further recommend that an annual audit of the Council’s hardware assets is undertaken.

**Observation**

Undertaking an exercise to identify and review the usage of laptop devices will help identify any laptops currently not on the Asset Register and will help in ensuring that all laptops meet the Council’s current security standard once they have been configured securely.

A process is currently underway to implement hard drive encryption on all Council supplied laptops. All senior management laptops now have hard drive encryption and the Councillors’ laptops are in the process of being completed. We, however, identified that service units were supplied with laptops some time ago and although there is no accurate record of these, it is estimated that there are approximately 40 of these laptops still in use. These do not have the current security features and the current process of encrypting laptops does not include the estimated 40 that are in use within the Council.

Where the Council is not aware of the usage of all laptops, there is a risk that older laptops in use do not have appropriate security installed on them. There is a further risk that in the event of loss or theft of the device that the Council is not aware of the data that is retained on devices and if this is protected by adequate security. Where this information is sensitive, there could be a risk of non compliance with Principle 7 of the Data Protection Act 1998.

**Responsibility**

John Worts – ICT Team Leader

**Management response**

Agreed

An annual review of Council equipment is conducted the last being completed in April 2011. The next review will be over March / April 2012.

The inventory will be extended this year to include Software and security running on all laptops and other ICT equipment.

April 2012

## **Recommendation 4: Security of Mobile Phones**

**(Priority 1)**

### **Recommendation**

The Council should consider a stronger and robust policy on the issue and use of mobile phones with the need for adequate security to prevent unauthorised access to information (email and data) in the event that the phone is mislaid or stolen.

### **Observation**

Enhancing security controls on mobile devices helps to ensure that specific standards have been established for portable devices. With the increase in the use of PDAs, Mobile devices and tablet PCs there is a need to enhance security controls to ensure that all users of these devices have appropriate security in place. Mobile devices by their nature are more portable and therefore more at risk to being lost, stolen or left in public places.

Currently, the issue of mobile devices is dependent on the procurement policy that is followed and several different types of phones are currently in use at the Council including Smart phones. Users are advised to set passwords/PINs on their phones but it is down to the individual to enforce this setting. If a phone is reported as stolen, it can be disabled so that no more emails are transmitted to the phone and the service provider will be requested to block the phone. Additionally, users have the ability to download documents which once downloaded are stored on the devices which may not be adequately protected.

Inadequate security and strong enforcement of policy over the security of phone and mobile devices could lead to data and information being accessible should the phone be stolen or lost.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

Agreed

All phones are password protected and ICT completed this work in the autumn of 2011. A further review of phone security will be conducted at the same time as the policy review (March 2012). Best practice will be used to ensure that the policy is up to date. Any new processes will then be implemented.

March 2012

## **Recommendation 5: Password Controls**

**(Priority 2)**

### **Recommendation**

Management should enhance the current password policies for the Corporate Network and for recommended practice within all Council applications. This should require a minimum password length of eight characters to be enforced and restrict the history of previous passwords that can be used to thirteen.

### **Observation**

Ensuring that adequate logical access controls are applied correctly to all systems and are enforced by the system helps to prevent unauthorised access through password guessing.

Although password policies on the network require complex passwords to be entered and that they are required to be changed every 90 days and the user account is locked out after three unsuccessful password attempts, the password length is currently set to six characters long and history of only six previous passwords is maintained.

Failure to implement strong password controls increases the likelihood that unauthorised users may gain access to the network.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

Agreed. To be implemented immediately

## **Recommendation 6: Formal user administration and leavers process (Priority 2)**

### **Recommendation**

ICT should develop a formal user administration procedure detailing the procedures and processes to be followed for the administration of user accounts. Additionally, a formal process should be introduced for a periodic review of user accounts. In addition, accounts that have not recorded any activity for 90 days should be disabled and any over 180 days should be deleted unless a valid reason has been provided for the account to remain active.

### **Observation**

Having a formal user administration process formalises the process for user management and authentication and provides a coordinated approach to the administration of user accounts. Performing a regular review of user accounts helps identify inactive accounts. The removal of unauthorised accounts helps prevent unauthorised access being attempted and gained to Council data.

Although there is a process for user administration and management, it is not formally documented. A leavers list is received from HR/Payroll and the user account is then removed. However, this only applies to permanent staff or those on long term contracts but does not cover temporary staff. Additionally, it is not easy to identify users that had not logged on for more than 90 days and whether these accounts should be active or disabled as the list provided contained more than 200 users that had not logged on for more than 90 days.

Failure to establish strong user management processes could mean that there is an ineffective process in place to manage user accounts and that accounts from old users are still retained exposing the system to unauthorised access.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

**Agreed.**

To be implemented as part of the policy review in March 2012.

**Recommendation 7: Audit Policy Settings and Logging**

**(Priority 2)**

**Recommendation**

The audit policy settings on the Windows network domain should be enhanced by applying the following suggested settings. These events should be reviewed as part of the audit log review process.

<b>Policy Items</b>	<b>Audited Events</b>
Account Management	Success, Failure
Directory Service Access	Success, Failure
Object Access	Success, Failure
Policy Change	Success, Failure
Privilege Use	Success, Failure
Process Tracking	Log failures of process events only
System Events	Success, Failure

Enabling some of these logs may have performance implications on the network and therefore the impact of all changes should be monitored to ensure that they do not have a detrimental effect to the required level of system performance.

**Observation**

Effective audit policy settings help to ensure that accountability can be established for both successful and failed user activities on the network.

Currently, the only user auditing (logging) in place on the network is that of user’s logon events. No other type of user activity is currently being logged. Additionally, the logs are only reviewed for ‘trouble shooting’ purposes. There is a requirement for effective audit logging to be in place for compliance with the Government GCSx Code of Connection.

Inappropriate audit policy settings or lack of auditing increases the risk that accountability cannot be established for activities on the system. Furthermore, there is a risk that the Council may not be in compliance with its GCSx Code of Connection requirements when it has not established strong audit policies.

**Responsibility**

John Worts – ICT Team Leader

**Management response**

Agreed

Following the evaluation of the effect these logs may have on the performance and the value of the log to GCSx compliance will be made before being implemented.

End of July 2012 completion.



## **Recommendation 8: Accounts with Non Expiry Passwords**

**(Priority 2)**

### **Recommendation**

A review should be carried out of all accounts whose passwords never expire and controls for these passwords changed to ensure that they are required to change their password in line with best practice.

Should there be an exception where its implementation may affect the operation of the service, this should be documented and its exception authorised by senior management.

### **Observation**

Requiring the use of passwords that meet leading practice standards enhances the integrity and security of the system and changing passwords on a regular basis helps to improve security and minimises the risk of unauthorised access.

There were 148 user accounts defined on the network whose passwords are set to never expire. Although the majority are service or system accounts or group mail boxes, we identified that there were still some individual accounts that were not required to change their passwords in line with system security settings.

Weak password controls can result in a loss of accountability for actions performed, and increases the risk of unauthorised, or inappropriate, access to systems and information resources.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

**Agreed** - A policy on exceptions to passwords will be developed. Some exceptions maybe needed for non-expiry accounts in order to run day to day IT operations. For exceptions a business case will need to be signed off by an Assistant Director.

Implementation will be with immediate effect.

## **Recommendation 9: Use of USBs (Memory Sticks)**

**(Priority 2)**

### **Recommendation**

The use of USBs (memory sticks) should be restricted by locking down (configuring) the PCs to only permit approved devices. Where there is a requirement for their use, only Council supplied encrypted devices should be used. Furthermore, we recommend that guidance is issued on the appropriate use of USB devices such as when they should be used and the type of data that may be loaded onto the device.

### **Observation**

Restricting the use of USB devices to only encrypted devices helps to ensure that only authorised and encrypted devices may be used to transfer Council data. Implementing guidance on the appropriate use of USB devices also helps to guide staff on what data is appropriate to load onto the device.

Non encrypted or personal USBs (memory sticks) can be used on Council devices to transfer Council data. The Council has recently purchased 200 memory sticks that will be encrypted and issued to Senior Managers, however, this will not prevent the use of non encrypted devices. Additionally, we are informed there is no guidance currently issued on how memory sticks should be used and the data that may be stored on the device.

There is a risk of rogue software being introduced in the Council's network which could seriously impact the Council's operation as evidenced in a number of recent incidents affecting local authorities. There is the additional risk of Council's data being lost or stolen through the use of unauthorised, unencrypted memory sticks.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

#### **Agreed.**

Corporately enforce the use of encrypted USB sticks of which authorisation will be performed at the Group Manager level. In addition we will prevent access to unauthorised devices.

Completion July 2012

## **Recommendation 10: Hardware Disposal Procedures**

**(Priority 2)**

### **Recommendation**

We recommend that a formal hardware disposal procedure is developed indicating the acceptable process for hardware disposal. Following agreement, this should be followed for the disposal of all Council equipment.

### **Observation**

A documented disposal procedure will formalise the process for disposal of hardware assets. This helps to ensure that the policy sets out when assets may be disposed of, by whom and who to contact if ICT asset disposal is required. This also helps to ensure that all hardware assets are disposed of according to the Council's standard process and have any information processed on the asset removed securely.

ICT have an informal process for the disposal of hardware.

Unless documented policies and procedures are established for the disposal of ICT hardware, there is a risk that the process is not universally understood that hardware could be disposed of without proper authorisation. There is also a further risk that if an uncoordinated process is followed for asset disposal that IT assets do not have all Council data removed from the asset when disposed of.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

Agreed

Asset Disposal policy will be reviewed and changes implemented.

Completion March 2012

**Recommendation 11: Legal Banner**

**(Priority 3)**

**Recommendation**

We recommend that the Council’s Legal Banner on accessing the Council network should be reviewed and updated to include the likely remedial action that could be taken in the event of non compliance with the relevant policies for usage within ICT.

Guidance should be sought from the Council’s legal officer for a suitable statement for inclusion.

**Observation**

An improved login banner will help ensure that those attempting to access the Council’s network are forewarned of unauthorised connections and assists the Council in legal litigation should the need arise. This would also provide the Council with recourse to the provisions of the 1990 Computer Misuse Act in the event of any non compliance.

When a user connects to the Council’s network, they are presented with a banner about the acceptance of the Council policies and where they may be found. However, it does not contain any legal statement/warnings in respect of unauthorised connection/access and the consequence of such unauthorised access.

Without a proper legal warning on any attempted access, it is possible that should an incident arise of unauthorised access then the Council may not be able to rely on its statement/warning banner in a litigation situation.

**Responsibility**

John Worts – ICT Team Leader

**Management response**

Agreed

Review the wording in the login banner against best practice will be completed and implemented.

End of February 2012 for completion.

## 2. Information Security and Governance

### Recommendation 12: Records and Information Management

(Priority 1)

#### Recommendation

We recommend that, as a minimum:

- The current Records and Information Management Policy is reviewed to ensure that it meets with the Council current requirements and usage of data;
- A periodic review is conducted to ensure that users and departments are complying with the policy, for example, on records and data management, retention and destruction;
- An exercise should be conducted to review and remove records that are no longer necessary (in compliance with the DPA) but keeping in mind any regulatory and legal requirements for retention; and
- A documented records disposal procedure should be developed which is available and distributed throughout the Council.

#### Observation

A strong Records and Data Management Policy will help in enforcing the Council's objective in records and data management. Periodic review of the document will help to ensure that users and departments are in compliance with the policy and the regulatory/legal requirements of the policy. A documented disposal procedure will provide guidance to users on the management and disposal of records.

The Council has a Records and Data Disposal policy in place. However, it was created in 2009 and is considered to be out of date. From the information provided, it is known that records and data exist dating back to 1995 that are no longer required or should have been archived. Data not removed or deleted is being retained and is probably in non-compliance with the 5<sup>th</sup> Principle of the Data Protection Act 1998.

There is a risk of non compliance with the Data Protection Act 1998 and a risk of unauthorised access to the data. Furthermore, the management of such data could put a strain on IT resources, to continue to manage the increased volume of data.

#### Responsibility

John Worts – ICT Team Leader

#### Management response

Agreed

We will review the current policy and update this using best practice.

End of March 2012 completion date.

## Recommendation 13: Data Sharing Protocols

(Priority 1)

### Recommendation

The Council should review its current approach to information sharing with other government agencies, third parties and private providers. This should ensure that:

- A review is carried out of the data sharing protocols document that is currently in place to ensure it is updated and reflects the requirements of sharing with third party organisations;
- All Departments should be required to formally identify who they share personal data with, the frequency and the form of information that is shared; and
- All users and departments should be advised of the revised protocols and to ensure that they are followed.

### Observation

A revised data sharing protocol will help ensure that it is in line with current practices and any legal/regulatory requirement. A review of the existing sharing agreements will help ensure that they are still valid and in line with current requirements. Furthermore, identifying all third parties that the Council shares data with would assist in helping to ensure that the Council was aware of the third parties to whom it shared data with and that appropriate monitoring and control systems are in place.

There is an Information Exchange Protocol document in place. Attached to this is a list of known contacts for the parties to the protocol. However, it is dated 2001 and has not been reviewed since that date. Furthermore, it is not clear from our audit discussions which areas in the Council have sharing agreements in place and for what areas they cover.

Failure to establish strong protocols for the management of sharing Council data would mean that the Council has not put adequate controls in place to protect Council data that is shared with third parties and other agencies. In the event that this data is lost or stolen, there is a risk that the Council could be liable to fines imposed by the Information Commissioner.

### Responsibility

John Worts – ICT Team Leader

### Management response

#### Agreed

We will review the Data Sharing protocol documentation and make amendments to the protocol where required.

End of May 2012 completion.

## Recommendation 14: IT Policies

(Priority 2)

### Recommendation

We recommend that a review of all the IT policies is conducted with a view to consolidating and creating an overarching Information Security Policy. Where appropriate, the Council should consider aligning its security arrangements with the guidance provided by ISO27001 the International Standard for Information Security.

Once revised and consolidated, the policy should be approved by senior management of the Council or the IT Governance Board or equivalent.

### Observation

Consolidating the existing information and IT related policies into a single document where it is appropriate will help to ensure that guidance related to ICT usage can be easily located in one area. This can assist in increasing awareness of the policy and assist in the maintenance of the policy. This also helps to ensure that the need to update related information in a range of policies becomes easier to perform and therefore can be reviewed on a periodic basis.

The Council does not have an overarching IT Security Policy in place. There are numerous policies in place covering ICT provision which does not assist in the update and management of the policies and in the awareness training required to be performed by users. All the policies were due for review in May 2011, however, since the departure of the Information Security Officer in January 2011, this review has not been performed.

Without an overarching policy, there is a risk that the message and the policy the Council is attempting to enforce may be missed or it is possible that this may result in confusing statements owing to the difficulty in maintaining consistency with a number of policies.

### Responsibility

John Worts – ICT Team Leader

### Management response

Agreed

Develop an overarching policy document for ICT Security in alignment to ISO 27001.

Competition March 2012

## **Recommendation 15: Security Officer Responsibility**

**(Priority 2)**

### **Recommendation**

We recommend that the Role and Responsibility of an Information Security Officer and a SIRO (Senior Information Risk Officer) is formally assigned and the officer appointed is provided with appropriate guidance relating the requirements of the role.

### **Observation**

Appointing and formally assigning the role of an Information Security Officer or a SIRO, will help ensure that information security is actively pursued in the organisation and that the person becomes a point of contact and information for any IT and Information security related matters.

Until January 2011, the Council had an Information Security Officer. However, since their departure, this role has been performed by the ICT Team Leader. This role has not been formalised nor has another officer been appointed to undertake this role in a much more active role. We also identified that a Senior Information Risk Officer has not been assigned to a Senior Management member within the Council

Failure to appoint an Information Security Officer could mean that the responsibility for ICT Security is not clearly defined and this means that appropriate guidance is not provided on Information Security issues. Unless the Council assigns the responsibility for Information Risk, there is a risk that the appropriate level of accountability has not been assigned within the Council.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

Agreed

Information Security Role will be defined within ICT but with links to the Legal Service. Implemented immediately.

The responsibility for the SIRO will be reviewed and will be formally assigned by February 2012. In addition the Council will look to set up an Information Governance Group with support from Legal Services and ICT.



## **Recommendation 16: Information Owner and Classification**

**(Priority 2)**

### **Recommendation**

We recommend that as part of records and Information Management Policy:

- Ownership of Information should be identified;
- Data and Information classification should be performed; and
- The Council should consider allocating the role of Records Manager to provide guidance on how records within the Authority should be maintained.

### **Observation**

Identification of information asset owners and the classification of the data according to its sensitivity will help ensure that information is provided with the security protection required in line with its sensitivity and that as part of the Records and Data Management Policy, management of the data is then made the responsibility of the data owners.

Appointment of a Records Manager will assist in the process of data and records management as defined in the policy and as required by the Council.

There is currently no formal Data Management Policy in place at the Council. There is no formal responsibility assigned to information ownership and a Records Manager has not been assigned. We also identified that there is no formal Information Asset ownership and that some system records extend for some time which may not be required or could be archived.

Failure to establish strong Data Management principles and ownership for Council information could mean the relevant accountability has not been established for data ownership within the Council. This could increase the risk that Council information may be retained for longer than required.

### **Responsibility**

John Worts - ICT Team Leader

### **Management response**

#### **Agreed**

A mini audit of the information asset owners will be undertaken. Following this classification of the data and information will be implemented.

Completion by the end of December 2012

There will be a project set up on information security which will include a plan on records and information management. The project will complete in April 2013.

## **Recommendation 17: Security of Laptops**

**(Priority 3)**

### **Recommendation**

The Council should consider the issue of cable locks to secure laptops and introduce a policy requiring users to use these when working on any off site location where there are no additional restrictions on entering office locations.

### **Observation**

Issuing cable locks for the use of Council devices would assist in allowing officers to secure portable PCs when working away from the office. This adds an additional deterrent from opportunistic theft.

Laptop users are not routinely issued with security cable locks and there is no policy in place to enforce physical security locks on laptops.

If additional processes are not established to provide for the security of laptop devices, there is a risk that laptops could be stolen due to opportunistic theft.

### **Responsibility**

Darren Kembel – Technical Support Assistant

### **Management response**

#### **Agreed**

Locks for PC's and laptops at remote sites has started and the role out is due to commence in January 2012.

Completion March 2012

## **Recommendation 18: Use of Emails – Monitoring**

**(Priority 3)**

### **Recommendation**

We recommend that periodic email monitoring and compliance checks are performed on the use of the Council's email systems to identify any instances of potential excessive usage during core working hours, this information should be routinely provided to management for information purposes.

### **Observation**

A periodic review will help ensure that use of the Council's email system by its staff (including temporary and contractors) is in compliance with its stated policy, i.e. not used other than for Council business.

Although there are email filters applied for the acceptable use of emails, there is no compliance check performed on acceptable email usage. Monitoring of email usage is only performed if it requested by a service manager.

There is a risk of the email system being used for excessive non Council business which could impact on service delivery.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

#### **Agreed**

When this is requested by a senior manager for the team they manage then we will conduct a review.

All Councillor laptops are being encrypted and offsite PC's are being encrypted this included all council off run sites. Additional license are being purchased to ensure that all offsite PC's and all Laptops are encrypted.

### 3. Observations and Recommendations from Site Visits

#### **Recommendation 19: File and Database Protection**

**(Priority 2)**

##### **Recommendation**

The Council should review the files and folders to certain private and confidential documents stored on remote site PCs and apply protection with the help of IT Services to restrict access to the databases to authorised officers only by use of passwords.

##### **Observation**

Applying strong password controls will help to ensure that files and folders are appropriately protected and access is only available to authorised users.

Review of settings on databases and spreadsheets during site visits identified that all documents did not have passwords applied to all documents stored on local drives of PCs.

Unless password settings are enforced for all databases where sensitive data is stored, there is a risk that in the event of loss or theft of the devices that Council data could be accessed.

##### **Responsibility**

Darren Kembel – Technical Support Assistant

##### **Management response**

Agreed

This is part of the encryption and lock down work that is being undertaken currently.

Completion for this work is March 2012.

## **Recommendation 20: Archiving of Records**

**(Priority 2)**

### **Recommendation**

The Council should review the existing process for storing Council records and especially for Children's data where appropriate documents should be destroyed securely when no longer in use and consideration should be given to scanning documentation to avoid physical copies of data being retained.

### **Observation**

Reviewing existing processes for retaining Council data and putting in place procedures for archiving data would help to ensure that the Council does not retain information longer than required and that its retention periods are in line with data protection legislation.

The current process is for electronic data to be retained until a child stops using Council facilities and existing data is then overwritten by changes made to the record. Paper copies of records are filed away and kept in the loft of the Chaulden Adventure Playground.

Failure to establish strong records management policies and procedures can mean that records are not subject to adequate retention periods and that the Council could be retaining information that is not required according to its policies and procedures.

### **Responsibility**

John Worts/Noele Pope – ICT Team Leader / Group Manager Legal Governance

### **Management response**

Agreed

We are reviewing current polices and ensuring that staff at remote sites are re-trained with regards to procedures on safe data handling.

March 2012

## **Recommendation 21: Recycle Bin on PCs**

**(Priority 3)**

### **Recommendation**

ICT should provide guidance to staff on how and how often to empty the local PC 'Recycle Bin' to avoid data being retained on Council PCs.

### **Observation**

Identification of the 'Recycle Bin' on the PC would allow the user to delete and restore files as necessary. This also means that items are not retained in the recycle bin for longer than necessary.

During our visit to a sample of Council sites we noted that the recycle bin is not visible on the PC from the user's profile. This means that recycle bins are not being emptied on a periodic basis to remove data from Council PCs.

Unless access to the recycle bin on the PCs is confirmed and users are reminded of the process to periodically clear the recycle bin there is a risk that data is not removed from the PC on a periodic basis.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

Agreed

We will develop a procedure note to go to all staff on the use of recycle bins and how to delete items from the PC.

Completion of this will be at the end of February 2012.

## **Recommendation 22: Data Protection Training**

**(Priority 2)**

### **Recommendation**

We recommend that the Council should review the approach used to train Council staff on Data Protection and safeguarding of data to ensure that those users who may process sensitive information are appropriately trained on how to handle personal data. Training and awareness processes should be documented to identify the procedures in place.

### **Observation**

The review of training provided to staff on data protection and information handling would show that the Council has put processes in place to train staff on effective and safe information handling. This assists in the Council being able to demonstrate the awareness that it has put in place over Council staff.

During our visits to Council sites, we identified that staff were not fully aware of how data classification should be applied and have not considered marking documents according to their sensitivity.

Failure to provide staff with effective training on data protection and information handling could mean that not all staff have the same level of awareness of safeguarding data especially in those areas where staff handle potentially sensitive information.

### **Responsibility**

John Worts – ICT Team Leader

### **Management response**

Agreed

The training package has been updated to reflect classification and marking.

Completed.

## **Recommendation 23: Confidentiality and Data Protection Statement**

**(Priority 2)**

### **Recommendation**

The Council should perform a review of all data collection forms used to obtain personal information to ensure that these contain a consistent Fair Processing notice. This should be applied to all forms and be approved by Legal Services.

### **Observation**

Having consistent statements applied to Council data collection documents helps to ensure that the Council has made residents and users of Council services aware of the reasons and purposes for data collection and sets out how the Council will safeguard personal data.

Review of a sample of information collection forms identified that there was not always a statement for the fair processing of data.

Unless the Council makes reference to the purpose of collecting information on data collection forms, there is a risk that residents and users of Council services are not made of aware of the purpose that Councils may use information supplied to them.

### **Responsibility**

Noele Pope – Group Manager (Legal Governance)

### **Management response**

Agreed

Data collection forms that are used will be obtained from all Group Managers and appropriate fair processing notices will be drafted by Legal Services and returned to Group Managers for inclusion in the forms.

This is a large task and completion is scheduled for June 2012.



**Recommendation 24: Generic use of Email Account****(Priority 2)****Recommendation**

All users at the Woodwell cemetery should be assigned with personal email accounts for conducting internal Council business, where a generic account is required this should be identified and users should be accountable for use of the generic account.

**Observation**

By allocating users with individual email accounts the Council helps to establish some accountability for usage.

Currently, a generic email account is being used by users at Woodwell Cemetery. The users do not have individual email accounts and there is no accountability for access on this account.

Unless individual email accounts are applied, there is a risk that accountability for the usage of this account cannot be established.

**Responsibility**

Kevin Bradley – Technical Support Officer

**Management response**





Agreed

This will be implemented by the end of February 2012.

## Appendix A – Reporting Definitions

### Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Level	Symbol	Evaluation Assessment	Testing Assessment
<b>Full</b>		There is a sound system of internal control designed to achieve the system objectives.	The controls are being consistently applied.
<b>Substantial</b>		Whilst there is a basically sound system of internal control design, there are weaknesses in design which may place some of the system objectives at risk.	There is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
<b>Limited</b>		Weaknesses in the system of internal control design are such as to put the system objectives at risk.	The level of non-compliance puts the system objectives at risk.
<b>Nil</b>		Control is generally weak leaving the system open to significant error or abuse.	Significant non-compliance with basic controls leaves the system open to error or abuse.

The assessment gradings provided here are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full' does not imply that there are no risks to the stated control objectives.

## Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
<b>Priority 1</b>	Recommendations which are fundamental to the system and upon which the organisation should take immediate action.
<b>Priority 2</b>	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
<b>Priority 3</b>	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
<b>System Improvement Opportunity</b>	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

## Appendix B – Staff interviewed

The following personnel were consulted:

Sally Marshall	Director of Finance and Corporate Services
Chris Gordon	Service Support Manager
John Worts	ICT Team Leader
Kevin Bradley	ICT Infrastructure Lead
Darren Kemble	ICT Technical Support Analyst
Mick Silvester	ICT Technical Support Analyst
Karl Yarham	ICT Technical Support Analyst
Chris Baker	Revenues and Benefits Manager
Jane Woodbridge	Children's Services Manager
Matt Rawdon	HR Team Leader
Graham Rayner	Chaulden Children's Adventure Playground Manager
John McRae	Berkhamstead Civic Centre
Roddy McGinley	Woodwell Cemetery Manager

We would like to thank the staff involved for their co-operation during the audit.

## Appendix C - Statement of responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system. The assurance level awarded in our internal audit report is not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

### **Deloitte & Touche Public Sector Internal Audit Limited**

**London**

**January 2012**

In this document references to Deloitte are references to Deloitte & Touche Public Sector Internal Audit Limited.

Registered office: Hill House, 1 Little New Street, London EC4A 3TR, United Kingdom. Registered in England and Wales No 4585162.

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte LLP, the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see [www.deloitte.co.uk/about](http://www.deloitte.co.uk/about) for a detailed description of the legal structure of DTTL and its member firms.

### **Member of Deloitte Touche Tohmatsu Limited**