www.oxford.gov.uk

OXFORD CITY COUNCIL

Report of: Head of Business Transformation and ICT Manager

To: Audit and Governance Committee

Date: 28th April 2009 **Item No:**

Title of Report: Information and Data Security Action update

Summary and Recommendations

Purpose of report: To report progress against the KPMG audit report on 'Review of Information and Data Security 2008/09' dated 7 November 2008

Key decision: No

Lead Member: Councillor Oscar Van Nooijen

Ward(s) affected: All

Report Approved by: Penny Gardner – Finance; Lindsay Cane, Legal and Democratic Services

Policy Framework: Transform Oxford City Council by improving value for money and service performance

Recommendation(s): That Members note the progress made.

Introduction

1. The KPMG 'Review of Information and Data Security 2008/09', reviewed by Audit and Governance Committee in November 2008, set out seven recommendations to improve information and data security arrangements in the Council. Two of the recommendation areas were priority one and five of the recommendations were priority two.

2. Progress has been made on all seven of the priorities and this report sets out that progress and the actions that are underway.

Progress to date on priority one recommendations

3. **Recommendation 1:** A more detailed information security policy has been prepared and implemented by updating the existing ICT Security Policy. This is under delegated approval received in 2003 from the CEB. An Information and Data Security procedure has also been developed, involving representatives from across the Council and has started to be implemented in sections since February, starting with urgent areas first. Data protection has been reviewed but no significant updates needed to be made.

4. **Recommendation 2:** An Information Security Officer has been appointed as part of the duties of the new ICT Manager, David Oakes. The Information Security Group has been formally brought together and meets monthly as part of the ICT City User group – a gathering of 15 ICT user representatives from all areas across the Council.

Progress to date on priority two recommendations

5. **Recommendation 3:** We have some formal data sharing protocols in place, particularly in one of the largest data sharing areas, Community Housing and Community Development. Work with Oxfordshire County Council and other partners is near to concluding the establishment of a general formal Data Sharing and Quality Protocol, which could be made use of by remaining areas of the council without formal protocols.

6. **Recommendation 4a:** A 69 page formal Data retention and Destruction procedure was drafted in 2005 and now that Information Asset owners have been formally appointed and an Information Group is in place, this will be updated and adopted in 2009.

7. **Recommendation 4b**: 14 secure confidential waste bins have now been installed and are in use in City Centre offices, with a further 6 being rolled out in April and current unsecure bins being withdrawn. City Homes have confirmed that their arrangements were already secure and City Works are buying in April, a cross-cut shredder for immediate shredding of their small amount of secure documents.

8. **Recommendation 5:** Induction training slides have been updated for this area and our ICT Manager / Information Security Officer will take part in the regular induction sessions for all staff from April onwards. The Government Connect project will also provide specific staff group training on information and data security arrangements, by 1 September 2009.

9. **Recommendation 6:** ICT has produced an incident management process as part of the Information and Data Security procedure and the Information Security Officer will coordinate any information incidents.

10. **Recommendation 7:** A formal back-up procedure has been produced as part of Information and Data Security procedure and forms part of the duties of ICT and ICT suppliers going forward.

Conclusion

11. Significant progress has been made on the recommendations made last year. We believe that all urgent work on the recommendations has been completed and remaining work will be completed by end of 2009.

Name and contact details of authors:
Ben Brownlee
Head of Business Transformation
Telephone: (01865) 25 2220
bbrownlee@oxford.gov.uk

David Oakes
ICT Manager
Telephone: (01865) 25 2503
doakes@oxford.gov.uk

Background papers:
ICT Security Policy, 25th March 2009

Oxford City Council – ICT Security Policy

Date of issue: 25 March 2009

Version: 5.1

1. Introduction

1.1 The purpose of this policy is to protect Oxford City Council's computer systems, network, devices and telephony ("the Systems or System") and associated information and data ("Information"), against threats, whether internal, external, deliberate or accidental.

1.2 It is the policy of the Oxford City Council ("the Council") to ensure that:

- All Systems and Information contained within them will be protected against unauthorised access.
- All members of the Council's staff, its contractors and councillors ("Users") must adhere to this policy.
- All breaches of security are reported to ICT and investigated by ICT.

1.3 ICT is responsible for:

- the integrity of all central computer systems and protecting the confidentiality of any Information contained within or accessible on or via these systems.
- all regulatory and legislative requirements regarding computer security and information confidentiality and integrity.

1.4 ICT is defined as the Council's Information and Communications Technology (ICT) Client Side Unit and / or its suppliers such as Oxfordshire County Council IT Services. Responsibilities are defined for the ICT Client Side Unit and its suppliers in the ICT Service Level and other Agreements.

2. Statement of Authority and Scope

2.1 This policy has been reviewed by User representatives and is intended to detail the rules of conduct for all Users of the computing and network facilities run on behalf of the Council.

2.2 All Users of the Council's computer facilities must:
a. abide by this policy and the Council's email and internet policy
b. assist the Council to comply with its legal responsibilities, relating to computer use including data protection, freedom of information, electronic communications, human rights, computer misuse, copyright and intellectual property.

3. Statement of Responsibilities

3.1a Individual Users are responsible for their own actions. The use of computing facilities by Users assumes and implies compliance with these policies without exception. Users of Systems have a duty to ensure the security, confidentiality and integrity of information.

3.1b Individual Users may not send Information of a "Restricted" classification or Confidential nature via electronic transfer to parties outside the Council without the express prior written permission from their Line Manager. All Information for transmission must be securely encrypted to the Council's encryption standard or higher, (as of 01/01/2009 this is at least 128bit AES or equivalent). The term "Restricted" is as defined by the Government Connect standard.

3.1c Individual Users may not take Confidential Information (whether such Confidential Information is "downloaded" onto disc, memory stick, paper or any other form of electronic or physical media) outside the Council's offices without first obtaining the prior written consent of their line manager on at least an annual basis. Where any such "downloaded" Confidential Information is held electronically it must be securely encrypted, at least to the Council's minimum encryption standard at the time (as of 01/01/2009 this is 128bit AES or equivalent). On any occasion when a user is authorised to take Confidential Information outside the Council's offices, the user will take all necessary precautions to ensure that the Confidential Information remains secure at all times, and is returned to the Council's safekeeping as quickly as possible.

3.1d Definition of Confidential Information for Users

Any data or information ("Information") that could reasonably be expected to cause damage or distress if disclosed or made public. This is **only** Information which could reasonably be expected to cause damage or distress if disclosed or made public about individuals and organisations and may be any type of Information, e.g. customer Information, personal Information, private Information, employee Information, or Information which is commercially sensitive.

For the avoidance of doubt, this definition **does not** include Users personal contact details held on mobile phones

Information and Data Security

3.1e Each significant category of Information (such as Benefits data) and each major system and data store is the responsibility of the relevant officer in the senior management structure of the Council as set out in section 4 of the Council's Constitution ("Information Asset Owners"), Information Asset Owners are accountable for the security of that data and the standards of confidentiality that are to apply to it. They may authorise officers they line manage ("Data Owners") to carry out these responsibilities on their behalf.

3.1f The Information Asset Owner is specified for each major system and data store. Access to each data store is limited to those needing such access to do their job. Each member of staff with such access is personally responsible for maintaining the confidentiality of the data to which he / she has access. The Information Asset Owner or Data Owner determines who should have access to data and the retention requirements. If data is to be deliberately destroyed, then the Information Asset Owner or Data Owner must ensure that destruction takes place in conditions compliant with the Data Protection Act.

3.1g Users who operate ICT Systems are responsible for the security of the System and programs, and must ensure that there is no unauthorised use of them.

3.1h Only Council provided equipment may be directly connected to the Council ICT network.

Failure to comply with Section 3.1 regarding Confidential Information by members of the Council's staff may be treated as gross misconduct.

3.2 Individual Users must:

- Be conversant with all security procedures and instructions issued for use with Systems
- Use the appropriate built-in security features of the System, e.g. passwords.
- Ensure that all computer account information pertinent to individuals, e.g. accounts and passwords, is managed accordingly and is not shared, written down or generally misused (see Section 5 - Computer Access).
- Report promptly to ICT any incidents that may have a security significance.

3.3 a. Human Resources is responsible for ensuring that all Heads of Service are aware of this policy and they in turn are responsible for informing their staff of this policy.
b. The Head of Legal and Democratic Services is responsible for ensuring that all Councillors are aware of this policy.

3.3 ICT is responsible for providing central security measures to protect the Council's computer Systems from external threats. This will include assessment of threats, provision of advice to services, provision of tools and software (e.g. virus scanners) and implementation of any security systems (e.g. firewalls, encrypted USB keys, encryption software).

3.4 ICT is responsible for the ICT Security Policy as a whole. Within each service area certain areas of ICT and computer security may be delegated to local support. This will be with full co-operation and support from ICT.

4. The Computing Environment

4.1 ICT plan, maintain and operate a range of central computing servers, core network, network switches, backup systems, and the overall network infrastructure interconnecting these systems.

4.2 The computing environment is defined as all Systems managed and overseen by ICT and all computing devices that can physically connect, and have been authorised to connect, to this environment. All are covered by this policy, including computing hardware and software, any Council related Information residing on these machines or accessible from these machines within the Council's network environment and any media such as floppy discs, CD-ROMs, DVD-ROMs, USB memory sticks and backup tapes that may at times be accessible.

4.3 All temporary and permanent connections via the Council's network, casual laptop docking points and the Remote Access Service are subject to the provisions of this policy.

4.4, Computing resources not owned by the Council or provided by ICT may not be directly connected to the Council's network, including all removal media such as USB keys.

4.5 ICT reserves the right on behalf of the Council to monitor, log, collect and analyse the technical content (e.g. network packets and data volumes) of all transmissions on networks maintained by both ICT and individual Services at any time deemed necessary for performance, security and fault diagnostic purposes. Any network monitoring will be performed in accordance with the relevant national and international legislation.

4.6 ICT Service Desk (x2111) is the initial contact point for Users who wish to obtain new accounts. For training in the use of computing systems Human Resources should be contacted.

5. Computer Access

5.1 All Users with valid user network access accounts may use computer systems at the Council. Accounts must not be shared, given away or offered for use to anybody else. User accounts issued are for the sole use of the individual to which they were issued.

5.2 All Users will be provided with an account username and initial password. Initial passwords should be changed on first login to one that is known to the user only. Passwords set by users should not be easy to guess, should be at least 8 characters long, and must include a mix of upper and lower case letters and digits.

5.3 If a password has not been changed for 90 days the user will automatically be forced by the Systems to do so.

5.4 If five failed attempts to enter a correct password are made the account will be locked for 15 minutes.

5.5 Computer accounts will be suspended on the final day of user's employment with the Council and deleted 30 days after this date. In exceptional circumstances accounts will be suspended immediately on the authorization of senior HR managers.

6. Physical Security

6.1 ICT provides a secure machine room with uninterruptible power supplies, fire protection, intruder alarm, air conditioning and remotely monitored environment.

6.2 In accordance with the Council's insurance policy and to prevent theft all desktop machines should be physically secured. Chains and locks for this purpose are provided by ICT.

6.3 Removable media such as USB keys, CDs and DVDs must be disposed of in a secure manner, within the Council's offices and rendered unreadable. The ICT Service Desk can provide guidance on appropriate disposal or they can perform this task for you.

7. General Computing

7.1 All Users are expected to make proper use of the Council's computing resources, including (but not limited to):

- Proper management of accounts and passwords.
- Proper management of login sessions, e.g. proper signoff or use of software locks when leaving the workstation unattended.
- Use of password protected screen savers or locking the PC by using 'Ctrl-Alt-Delete' and selecting the 'lock computer' option within Task Manager, when left unattended
- Log-off and shut down the PC at the end of the working day. If the PC must be left on and logged in for operational reasons please inform ICT. Failure to do so will result in the PC being shutdown automatically by software called "Nightwatchman" in accordance with this policy and our energy-saving initiatives.
- To comply with software copyrights and licence restrictions. In general software and datasets should not be used for commercial purposes unless specifically licensed for such use.
- Proper management of confidential information and data.

8. Internet Access

8.1 The Council's network interconnects with the worldwide web via a firewall. ICT manage the firewall with the objective of protecting the Council's network and systems from unauthorised or illegal access or attack from the external environment. No internet access should take place from any device attached to the Council network other than via the above connection unless specifically authorised and configured by ICT.

9. Intranet Access

9.1 When sensitive, confidential or personal information is recognised as such it must not be distributed further as per this policy and the Email and Internet Security Policy.

10. Remote Access

10.1 Users connected to the Council's network via Remote Access connections are subject to the same rules and regulations, policies and practices as if they were physically on Council property.

10.2 ICT provides the only remote service that can be used, which is a secure, encrypted and authenticated service. All connections to this service will be logged. No other remote access service shall be installed or set up, including single modems connected to servers or workstations. Any active dial-in links found to be in existence will be removed from the network unless their use has been previously and specifically agreed with ICT.

11. Wireless Networks

11.1 Direct wireless connection to the Council's network from any device is only allowed if specifically authorised and configured by ICT.

11.2 Wireless connection to the internet or any external network from any device physically connected to the Council's network is not allowed.

12. Email

12.1 Email use is covered by a separate policy, the Email and Internet Policy. All users of email facilities supplied by Oxford City Council will abide by this policy.

13. Internet

13.1 Use of the Internet is covered by a separate policy, the Email and Internet Policy. All Users of Internet facilities supplied by Oxford City Council will abide by this policy.

14. Central File Servers

14.1 All Users have access to the centrally-managed file servers. These servers are secured and tape copies for the purpose of back-up are sent off-site daily by ICT.

14.2 Business critical servers are protected by disaster recovery arrangements so that in the event of catastrophic loss the data can be recovered.

14.3 Local disk drives on PCs, laptops and other devices (e.g. the 'C:' drive) are not backed up. As data stored on these drives cannot be recovered (in event of hardware loss or failure) they should not be used to store important data.

15. Anti Virus Security

15.1 ICT is responsible for protecting the Council's Server and desktop computers from Virus attack by the use of antivirus software.

15.2 It is the responsibility of each individual user to take all reasonable steps to protect the integrity of desktop and portable devices, and specifically not to:

- Knowingly use virus infected media (Floppy disks, CDs, Memory sticks USB keys and the like,) on any Council owned device or any other device connected to the Council's network

- Tamper, interfere with or attempt to remove the Anti Virus software installed on any Council owned device

16. Computer Software and Copyright Law

16.1 Unlicensed duplication or use of any software programme is illegal and can expose the Council to civil and criminal liability under copyright law. Therefore Users must not:

- Install any software on to any Council owned device without the prior written permission of ICT.

- Copy any software from any Council owned device, for any purpose, without prior written permission from ICT.

16.2 All software installed on Council owned devices must be recorded in the Software Inventory Register managed and maintained by ICT. The original software licence documentation and Software licence key(s) must be retained by ICT.

17. Relevant Legislation

Data Protection Act 1998

Freedom of Information Act 2000

Electronic Communications Act 2000

Regulation of Investigatory Powers Act 2000

Human Rights Act 1998

Computer Misuse Act 1990

Related Policies

Oxford City Council's Email and Internet Policy

18. Document History

Version	Replaces	Date
0.1 Draft	None	01/02/03

Reason for Issue – first draft.

Version	Replaces	Date
0.2 Draft	0.1 Draft	10/02/03

Reason for Issue – updated initial draft to take into account additional research by the document author.

Version	Replaces	Date
0.3 Draft	0.2 Draft	18/02/03

Reason for Issue - produced after consultation with Core Systems and Enabling Technologies teams.

Version	Replaces	Date
0.4 Draft	0.3 Draft	19/04/03

Reason for Issue – produced after consultation with Business Systems, Agresso Administrators, City Works IT administrators, Academy Administrators.

Version	Replaces	Date
0.5 Draft	0.4 Draft	02/05/03

Reason for Issue – produced after further discussions with the Technical Development Manager.

Version	Replaces	Date
1.0	0.5 Draft	10/05/2003

Reason for Issue – endorsement by the Chief Executive, and page formatting for the OCC Intranet service.

Version	Replaces	Date
1.1	1.0	14/11/2003

Reason for Issue – amended and approved by Joint Consultative Committee

Version	Replaces	Date
1.1	1.0	14/11/2003

Reason for Issue – amended and approved by Joint Consultative Committee and by the Executive Board on January 5th 2004. Executive Board delegated authority to future updates to Business Systems.

Version	Replaces	Date
2.0	1.1	16/05/05

Reason for Issue – annual update by Business Systems.

Version	Replaces	Date
3.0	2.0	10/04/06

Reason for Issue – annual update by Business Systems.
New sections 5.4 and 5.5 added.

Version	Replaces	Date
3.1	3.0	20/10/06

Reason for Issue – update to section 5.2 for new password policy.

Version	Replaces	Date
4.0	3.1	15/03/07

Reason for Issue – annual update by Business Systems.

Version	Replaces	Date
5.0	4.0	21.02.08

Reason for issue – annual revision by Business Systems

Version	Replaces	Date
5.1	5.0	25.03.09

Reason for issue – update for Information and Data security policy addition within this ICT Policy and creation of the ICT Client Side Unit / ICT partnership, by David Oakes, ICT Manager, Lindsay Cane, Legal & Democratic Services and Ben Brownlee, Head of Business Transformation