Oxford City Council – IT Security Policy

Date of issue : February 2008

Version : 5.0

1. Introduction

1.1 The purpose of this policy is to protect Oxford City Council's computer systems, network and all data contained within, or accessible on or via these computer systems from threats whether internal, external, deliberate or accidental.

1.2 It is the policy of the Council to ensure that:

- All central computer systems and information contained within them will be protected against unauthorised access.
- All members of staff and Councillors are aware that it is their responsibility to adhere to this policy.
- All breaches of security are reported to and investigated by Business Systems.
- The execution of its normal duties is not significantly degraded.

1.3 Business Systems 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.

2. Statement of Authority and Scope

2.1 This policy has been approved by Unison and is intended to detail the rules of conduct for all staff and Councillors of Oxford City Council who use the computing and network facilities run on behalf of the Council.

2.2 All members of staff and Councillors, who agree and abide by this policy and the Council's Email and Internet Policy are entitled to use appropriate and approved computing facilities at all times when the network is available.

2.3 The Council complies with all its current legal responsibilities including Data Protection, Freedom of Information, Electronic Communication and Human Rights, Computer Misuse, Copyright and Intellectual Property.

3. Statement of Responsibilities

3.1 Individual users are responsible for their own actions. The use of computing facilities by individuals at the Council assumes and implies compliance with these policies without exception. Every user of computer services has a duty to ensure the security, confidentiality and integrity of information in the system.

3.2 Individual Users must:

- Be conversant with all security orders and instructions issued for use with the system, e.g. this policy.
- 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 Business Systems any incidents that may have a security significance.

3.3 Human Resources and the Members' Services Officer are responsible for ensuring that all Business Managers and Councillors are aware of this policy and they in turn are responsible for informing their staff of this policy.

3.3 Business Systems are responsible for providing central security measures to protect the Council's computer systems and networks from external threats. This will include assessment of threats, provision of advice to departments, provision of tools and software (e.g. virus scanners) and implementation of any security systems (e.g. firewalls).

3.4 Business Systems are responsible for the IT Security Policy as a whole. Within each Business Unit certain areas of IT and computer security may be delegated to local support. This will be with full co-operation and support from Business Systems.

4. The Computing Environment

4.1 Business Systems 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 central computing resources and network infrastructure managed and overseen by Business Systems 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 data 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 Subject to the prior approval of Business Systems, computing resources not owned by the Council may be connected to the Council's network. However, all such resources must function in accordance with Council regulations governing the use of computing resources.

4.5 Business Systems 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 Business Systems and individual departments 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 The Business Systems 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 should 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 system 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 Business Systems 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 Business Systems.

6.3 Removable media such as CDs and DVDs must be disposed of in a secure manner. The Business Systems 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 reasonable efforts towards ensuring proper use of the Council's computing resources. Such efforts include (but are certainly 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.
- 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 Business Systems. 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.
- Respect of 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 sensitive information.

8. Internet Access

8.1 The Council’s network interconnects with the worldwide web via a firewall. Business Systems 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 Business Systems.

9. Intranet Access

9.1 When sensitive, confidential or personal information is recognised as such it should not be distributed further.

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 Business Systems provide 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 Business Systems.

11. Wireless Networks

11.1 Wireless connection to the Council's network from any device is only allowed if specifically authorised and configured by Business Systems.

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.

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 Business Systems 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 etc,) 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 staff and Councillors must not;

- Install any software on to any Council owned device without the permission of Business Systems.

- Copy any software from any Council owned device, for any purpose, without permission from Business Systems.

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

17. Related Documentation

Data Protection Act 1998

Freedom of Information Act 2000

Electronic Communications Act 2000

Regulation of Investigator Powers Act 2000

Human Rights Act 1998

Computer Misuse Act 1990

HMSO Copyright

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