Derby City Council

Personnel Committee
7 July 2016

ITEM 8

Report of the Director of Governance and Monitoring Officer

Laptop, Desktop and Tablet Device Security Policy

SUMMARY

1.1 This policy sets out the rules that apply to the physical and local security of Council owned and managed laptop, desktop and tablet computers.

1.2 The report seeks to introduce a revised and updated policy that aims to make staff aware of their responsibilities and the things they should – or should not – do to work safely and securely.

RECOMMENDATIONS

2.1 The policy will raise awareness on good information security practices when using Council owned and managed laptop, desktop and tablet computers.

2.2 To adopt the revised policy that was agreed with the Trade Unions at CoSWP on 10 June 2016.

2.3 To promote this revised policy through the In Touch and Manager's Briefing cascade process.

2.4 To agree that future changes to the policy, for example, to amend named officers and/or to bring these up to date do not need formal ratification. Any changes that alter the nature or intent of the policy, for example, when Bring/Use Your Own Device policy is agreed the changes will need to be incorporated.

REASONS FOR RECOMMENDATIONS

3.1 It is important that Derby's citizens are able to trust the Council to act appropriately when obtaining, holding and sharing information when using the authority's facilities. It is also important that information owned by other organisations which is made available to the Council under secondary disclosure agreements is treated appropriately. By understanding and implementing our responsibilities we can make sure our citizens have trust and confidence in the way they can access our systems and the way we manage, store, share and use our information assets.

3.2 The policy is explained in simpler terms and the document has been shortened and items removed or amended to reduce the 'technical jargon' that staff do not want or need to know.

3.3 The Information Governance Board must review all policies and authorise all changes.

They would recommend formal ratification of policies where the nature or intent had been amended. If committee approval is not required the policy would be published and the committee informed at the next meeting.

SUPPORTING INFORMATION

4.1 Maintaining compliance with third party Codes of Connection for example the Public Services Network, a programme designed by the UK Government to create one ICT network for all UK public sector organisations.

4.2 Applying the International Standard ISO/IEC 27001:2013 standard specification for Information Security Management which defines Information Security as protecting three aspects of information:

- *confidentiality* - making sure that information is accessible only to those authorised to have access
- *integrity* - safeguarding the accuracy and completeness of information and processing methods
- *availability* - making sure that authorised users have access to information and associated resources when required.

4.3 Applying the seventh principle of the Data Protection Act:

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

OTHER OPTIONS CONSIDERED

5.1 Information security is not an option. We are all required to maintain a minimum level of Information Security to maintain our legal and contractual obligations. Defined and approved policies and standards of information security must be implemented.

5.2 Failure to issue a policy increases the risks which, should a data breach occur, lead to action against the Council for not having relevant controls and a clear policy.

This report has been approved by the following officers:

Legal officer	Janie Berry - Director of Governance and Monitoring Officer
Financial officer	Not applicable
Human Resources officer	Diane Sturdy
Estates/Property officer	Not applicable
Service Director(s)	Nick O'Reilly – Director of Digital Services
Other(s)	Richard Boneham – Head of Governance & Assurance

For more information contact:	Angela Gregson 01332 642670 angela.gregson@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications Appendix 2 - Organisation and Governance: Remote and Mobile Computing Policy v2.0 Appendix 3 – Equality Impact Assessment, see item 5 on the agenda

IMPLICATIONS

Financial and Value for Money

1.1 There are no direct financial implications unless a data breach caused the Council to be unable to fulfil its role and/or resulted in a fine from the ICO.

Legal

2.1 There are no direct legal implications unless a data breach caused the Council to be accountable to the ICO.

Personnel

3.1 Every person is responsible and accountable for putting into practice these policies, standards and procedures.

3.2 The policy will apply to all persons having legitimate access to Council systems and data. It has gone through the agreed consultation procedures with the Trade Unions.

IT

4.1 The IT implications are covered in the body of the report.

Equalities Impact

5.1 None

Health and Safety

6.1 None

Environmental Sustainability

7.1 None

Property and Asset Management

8.1 None

Risk Management

9.1 A data breach must be reported for it to be recorded and investigated.

Corporate objectives and priorities for change

10.1 The Council aims to be a leading digital organisation, with a modern way of working that facilitates staff, customers and partners. It endeavours to try and ensure that the computer network is safe and secure for staff and its customers.

10.2 The Council's objective is to reduce the risk of information security incidents and be able to demonstrate to the citizens and businesses of Derby that we collect, handle and store their information securely.

Appendix 2

Information Systems Governance:

Laptop, Desktop and Tablet Device Security Policy

Document owner	Information Systems Client Team Manager
Document author	Nick O'Reilly
Document date	January 2016
Version	2.0 Draft for review
Document classification	Official
Document distribution	Published via the Council Intranet
Next review date	01/06/2017

Version Control

To make sure you are using the current version of this policy please check on iDerby or contact Information Governance when using printed copies.

Version Number	Date	Author	Reason for Version
No ref	March 2013	Elphia Miller	Last updated version on iDerby
2.0	January 2016	Nick O'Reilly	Updated

Document Approval

Job Role	Approvers Name	Date Approved
Director of Digital Services	Nick O'Reilly	28/1/16
Information Governance Group	Head of Governance and Assurance – Richard Boneham	28/1/16
Personnel Committee		
Corporate Joint Committee		
Conditions of Service Working Party	Director of Governance and Monitoring Officer – Janie Berry	10/6/16

Please tell us if you need this in large print, on audio tape, computer disc or in Braille.
You can contact Ann Webster on 64 3722, Minicom: 01332 64 0666 or Text Relay: 18001 01332 643722

Contents

1. Introduction

This policy sets out the rules that apply to the physical and local security of Council owned and managed laptop, desktop and tablet computers. If and when a Bring/Use Your Own Device policy is agreed it will set out the rules for non-council owned devices.

2. Scope

This policy applies to all employees of the Council, elected members, contractors, agents, partners and temporary staff who have authorised access to Council IT systems who can work remotely and use mobile computing equipment. This includes staff that access Council email from smart-phones.

3. Physical Security (Office, Home and Elsewhere)

Devices not secured to an office desk must be locked away overnight and/or when not in use; they can be locked in personal lockers or secure team storage.

Devices kept at home should be locked away when not in use if at all possible, and must be stored as securely as is possible when the home is empty.

Computers must never be left unattended when in other party's premises or when travelling to or from site. If travelling by car, devices can be left locked in your car

boot provided this is not visible for short breaks but should not be left there overnight.

4. Device Logical Security

All computers are issued with prevailing security standards and users must not tamper with these pre-set security measures that include:

- Mandatory power on/boot-up passwords before the device can be accessed
- Mandatory encryption of the hard disk and of any portable memory stick inserted into the device
- Inactivity timeout security that both locks the screen and forces entry of a password after a set period of time (15 minutes)
- Mandatory timed updates of malware protection

5. Device and Network connectivity

Before any computer can be used on the network we establish some network security settings that allow remote management and administration of the device and management of security patches and malware updates.

It is a requirement that all computers are connected to the network every week to receive the latest updates.

If staff are on long term absence their manager needs to ensure that any laptop or tablet device or any desktop computer is connected to the network, powered on and logged on in order to receive such updates. They should be left connected (but locked from user access) between 9:00am and 5:00pm to ensure the updates are received.

If a device has not been connected for 30 days this is flagged centrally and if it has still not been connected for another 30 days the device will be barred from the network in order to meet mandatory security compliance regulations.

Any devices so barred will incur a re-connection fee of £300, this reflects the cost incurred in undertaking a full security check and to update all the required security protection files.

6. User/Usage Security

All staff have responsibilities for the security of devices and data held in accessible form on those devices; these include:

- Use of a mandatory complex password to log on (8 characters with 1 upper case, 1 lower case, 1 number and 1 other keyboard character)
- Passwords that age and that have maximum re-try limits after which an account will lock (and need a password reset)
- Not writing down the password to machine power on/boot or the network log-on password, and never sharing your password with anyone else (Not even a work colleague)
- Only storing data on network drives as configured or on encrypted portable media (e.g. Council supplied memory sticks)

- Not forwarding Council emails or files to a personal email address
- Reporting promptly any device that is lost or stolen and/or any suspected email or virus alert
- Not installing or downloading any software even if prompted by internet pages or pop-up windows (all software must be installed by the Information System department who will undertake security checks first.)

7. Using the Remote Access Citrix Gateway

We permit the use of an approved secure remote gateway to access council emails and file systems remotely, this is currently the only way you can access such information from a non-Council computer.

This gateway can be installed on your own computer by following simple instructions provided on iDerby; it will not allow you to make local copies of any email or any council file.

8. Responsibilities and Accountabilities

8.1 The Head of Governance & Assurance has responsibility for defining the Council's information security policies, standards and procedures which are approved by the Information Governance Board. Every employee, and in particular line managers, is responsible and accountable for putting into practice these policies, standards and procedures.

8.2 ***Security is not an option.*** We are all required to keep a minimum level of security to meet our legal and contractual obligations; and data sharing protocols with our partners.

8.3 For the avoidance of doubt this policy sits under both the Employee Code of Conduct and the Information Security Policy and as such any work using computer devices must be consistent with those.

9. Compliance with Laptop, Desktop and Tablet Device Security Policy

9.1 The Head of Governance & Assurance is responsible for monitoring compliance with this policy.

9.2 If employees knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action in accordance with the Employee Code of Conduct.

10. Other Relevant Policies, Standards and Procedures

These can be found on iDerby or contact the Information Governance team.

11. Contact Details

Please contact the Council's Head of Governance & Assurance or anyone in the Information Governance team with enquiries about this or any other referenced policy, procedure or law.

Email to: information.governance@derby.gov.uk
Telephone: 01332 640763