Derby City Council

Personnel Committee
7 July 2016

ITEM 9

Report of the Director of Governance and Monitoring Officer

Remote and Mobile Computing Policy

SUMMARY

1.1 This policy has been developed to promote good information security practices outside the boundaries of Council premises – including remote and home working. The security issues in this policy relate to the physical security of mobile computer equipment and mobile storage devices, including the data held on them.

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 outside of Council premises whilst ensuring confidentiality of data.

RECOMMENDATIONS

2.1 The policy will raise awareness on good information security practices outside the boundaries of Council premises – including remote and home working.

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, changing the guidance on bring/use your own device.

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

Appendix 1

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

Organisation and Governance:
Remote and Mobile Computing Policy

Document owner	Richard Boneham, Head of Governance & Assurance
Document author and enquiry point	Angela Gregson
Date of document	January 2016
Version	2.0
Document classification	Official
Document distribution	Published via iDerby website
Review date of document	January 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.

Date Issued	Version	Status	Reason for change
December 2013	1.0	Issued	
	2.0	Draft	General review and update

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

The Council supports secure and managed remote and mobile computing and this policy establishes the framework under which can be undertaken.

This policy has been developed to promote good information security practices outside the boundaries of Council premises – including remote and home working. The security issues in this policy relate to the physical security of mobile computer equipment and mobile storage devices, including the data held on them.

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. Remote Access and Security

When working remotely all staff must:

- Use computer devices provided by the council that have been configured with the required security

- If using their own device connect via the approved remote access gateway that prevents data being copied form the council network to the local device
- Only use encrypted memory sticks
- Use network connection utilities (such as Virtual Private Network access or thin client access) provided and approved for council use
- If identified as accessing sensitive data that requires dual factor authentication have such tools installed and configured
- Ensure any local (home) wireless (Wi-Fi) network has been secured and is not open
- Take care when working in public places, consider if the screen is visible and what the nature of their data is – if this is confidential or sensitive then it may not be appropriate in a public place
- Lock or shut down their computers when not in use in the same way as office computers; all devices should be set to auto lock requiring a password after 15 minutes of inactivity.
- Leave such devices in secure locked places when not in use and not leave them unattended or insecure in the home, in a public place or in a motor vehicle.

4. Bring/Use your Own Device

The ability to use your own computer device currently only exists if using a secure thin client (Citrix) gateway connection. We are exploring other forms of Bring your Own Device security and this may be extended.

The ability to use your personal smartphone to receive Council emails is only permitted if your smartphone has been configured with strong password security (more than the 4 digit pin code) and the email has been configured by the Information Systems department.

If using your own device or a Council provided device at home you must **not** copy any data to the local drive and you must not allow any family or household member to access the Council data in that device.

5. Lost or Stolen devices

If your Council device is lost or stolen this must be reported immediately to both your line manager and via the IT service desk.

If your own device is lost or stolen you must also report this immediately to the IT service desk that will use mobile device management tools to lock and/or delete any Council data.

If your smartphone is lost or stolen you must report this immediately to the IT service desk for Council provided phones or to your mobile phone operator for personal devices and ask that the phone is locked.

6. Responsibilities and Accountabilities

6.1 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.

6.2 ***Information 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.

6.3 For the avoidance of doubt this policy sits under both the Employee Code of Conduct and the Information Security Policy and as such any remote or mobile computing must be consistent with those.

7. Compliance with the Remote and Mobile Computing Policy

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

7.2 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.

8. Other Relevant Policies, Standards and Procedures

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

9. 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