Derby City Council

Personnel Committee
7 July 2016

ITEM 10

Report of the Director of Governance and Monitoring Officer

Network User Policy

SUMMARY

1.1 This policy is to explain the actions that all persons that access the Council's data and use the Council's technology to do their job must follow to ensure security of data and systems.

1.2 The report seeks to introduce a new policy that aims to make staff aware of their responsibilities and the things they should – or should not – do to ensure we comply with the Data Protection Act and that we do not commit any offences under the Computer Misuse Act 1990.

RECOMMENDATIONS

2.1 The policy will raise awareness on the security of passwords, storage of information and the use and misuse of data on the Council's systems. It will also reinforce the Council's Malware Policy.

2.2 It will advise all persons using the Council's IT systems of unacceptable actions regarding the handling and use of data held by the Council.

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

2.4 To provide a mandatory e-learning programme as required by the Information Commissioners Office (ICO) to ensure all accessing Council computers understand and act to minimise the risks of infections.

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

2.6 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 length or composition of network passwords.

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 simple terms and the document has been written without ‘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: Network User Policy 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

Organisation and Governance:
Network User Policy

Document owner	Richard Boneham, Head of Governance & Assurance
Document author and enquiry point	Angela Gregson
Review date of document	December 2015
Version	V1.0
Document classification	Official
Document distribution	Internal
Document retention period	Until date of next review
Next document review date	1 April 2016

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
	1.0	Draft	New policy

Document Approval

Job Role	**Approvers Name**	**Date Approved**
Director of Digital Services	Nick O'Reilly	28 January 2016
Information Governance Group	Head of Governance and Assurance	28 January 2016
Personnel Committee		
Corporate Joint Committee		
Conditions of Service Working Party	Director of Governance and Monitoring Officer	10 June 2016

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 and Scope

The Council provides access to Information Systems and IT facilities for business purposes. Employees have access to the latest data and technology on the basis that these are necessary tools to help you do your job faster and more efficiently. Likewise, access to email and iDerby - the Council's Intranet - are standard tools available to anyone provided with a computer connected to the Council's network.

2. Definitions

- The Council – Derby City Council
- Should – indicates a recommendation - good practice
- Must – indicates that something has to be done to satisfactory requirements – mandatory
- Must not – indicates that something must not be done - mandatory.

3. Network Policy

3.1 When setting up network passwords employees must use a minimum of 8 characters including at least three of the following:

- one upper case character (A-Z)
- one lower case character (a-z)
- one numeric (0-9)
- one special character (e.g. !£$%&*)

3.2 Keep all passwords secure and change them regularly. Do not reveal, write them down or share them with anyone.

3.3 Employees **must not** use or encourage others to use anyone else's personal ID and password to log onto a PC, the network, individual system or email.

3.4 It is a criminal offence under the ***Computer Misuse Act 1990*** to access a computer system without authority to do so. Employees must not access or attempt to access any pc, network, business application, file or record without the explicit permission of Derby City Council.

3.5 Employees must not store personal, non-business related information on network drives or servers. If IT Support identifies non-work related personal information, e.g. family photos, held on any server or network drive as part of a storage audit they will notify Information Governance and they will be removed.

3.6 Employees must not view, amend, or delete any record of any individual service user known personally to the employee or on the request of someone known personally to the employee unless authorisation has been sought and given by line managers. If you realise you are accessing a record of a person known to you, you should stop and report this to your manager unless the issue is time critical (in which case you should inform them as soon as possible).

3.7 Employees must store all business related information on shared team drives. This ensures that all your files are accessible to your team and line manager.

3.8 If you are unexpectedly away from the office access may be given to your line manager to view your mailbox for incoming mail items. This will be for urgent, business reasons only.

3.9 When an employee leaves or transfers the line manager must confirm with the employee that all their business related information is on the shared team drives.

3.10 Employees must **not** connect non-Council owned equipment or mobile devices to the corporate network.

4. Malware Protection

Everyone has a responsibility, and a duty of care to our customers to protect the data we hold and as such to make sure that the Council network and IT systems stay virus free by complying with the Council's Malware Policy.

In summary:

- All mobile devices **must** be connected to the network at least once every **20** days to make sure malware software is up to date
- never open email attachments from an unknown source
- check all removable storage – such as, CD's, DVD's and pen drives for viruses . If you are unsure how to do this please contact IT Support.
- always report incidents on virus infection to IT Support and the Council's Information Governance Manager.

5. Responsibilities

Managers are responsible for ensuring that this policy is communicated to all employees and that it is adhered to. They must:

- ensure this and other Information Governance policies are part of the induction process and probation periods cannot be completed without passing the relevant Information Governance courses.
- ensure the level of access for staff is appropriate for their role and business purposes
- ensure that authorised users are given appropriate training and are fully briefed in the legitimate and lawful use of the systems in accordance with the standards set down in this policy
- comply with Council procedures for removing or amending the access rights of their staff who change jobs or leave the Council.

6. Compliance with the Network User Policy

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

6.2 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.

7. Other Relevant Policies, Standards and Procedures

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

8. 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