Derby City Council

Personnel Committee
14 January 2016

ITEM 7

Report of the Strategic Director of Governance

Information Security Policy

SUMMARY

1.1 Information Security covers the safekeeping of all forms of information to protect its confidentiality, integrity and availability.

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 prevent data breaches.

RECOMMENDATIONS

2.1 The policy will raise awareness on the security of electronic and non-electronic data. Staff should be aware that information security refers to all data including anything that has been printed or written.

2.2 To adopt the revised policy that was agreed with the Trade Unions at CoSWP on 8 November 2015.

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

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 agree that future changes to the subset of policies such as malware and email use, 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 policy to no longer allow personal use of email would need ratification but adding web mail or instant messaging services would not.

REASONS FOR RECOMMENDATIONS

3.1 It is important that Derby's citizens are able to trust the Council to act appropriately when obtaining and holding information and 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 current policy was agreed in September 2013 although it has had references to, and email addresses, for a previous post holder removed in the interim. It has been updated to take into account current practices and generic contacts added which will allow for staff changes.

3.3 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.

3.4 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 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 an updated 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	Gordon Stirling - Director of Strategic Services and Organisational Development
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: Information Security Policy

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.

2.2 The policy highlights a level of responsibility for line managers to ensure all persons have authorised use of the Council's IT systems and that they are aware of the management of non-electronic information.

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: Information Security Policy

Document owner	Richard Boneham, Head of Governance & Assurance
Document author and enquiry point	Angela Gregson
Date of document	September 2015
Version	9.0
Document classification	Official
Document distribution	Published via the Council website
Review date of document	July 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
July 2012	8.0	Issued	General review and update
September 2013	8.1	Issued	General review and update to include references to CJSM
February 2015	8.2	Issued	Removal of references to the Information Governance Manager.
September 2015	9.0	Draft	General review and update

Document Approval

Job Role	Approvers Name	Date Approved
Director of Digital Services	Nick O'Reilly	
Information Governance Group	Head of Governance and Assurance	
Chief Officer Group		
Personnel Committee		
Corporate Joint Committee		
Conditions of Service Working Party	Director of Governance and Monitoring Officer	9 October 2015

Contents

1. Introduction

The purpose of information security is to protect the highly valued information assets of the Council. The 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. It also shows a commitment by the

Council to process information in line with relevant legislation and compliance requirements.

2. Definition

2.1 The International Standard ISO/IEC 27001:2013 standard specification for Information Security Management 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.

2.2 Information Security is put into practice through appropriate controls, which will be a combination of policies, procedures, standards, guidelines, common sense and physical or logical (hardware/software) measures.

3. Scope

3.1 Information is in many forms. It can be:

- stored on computers and devices e.g. memory sticks
- sent across networks
- printed out
- written
- spoken
- visual

3.2 Information Security covers the safekeeping of all forms of information, held on all types of media, to protect its confidentiality, integrity and availability.

3.3 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.

4. Direction and Vision

The Council's vision is citizen-centred to enhance their participation in and access to local and national government services. We want Derby's citizens, visitors, voluntary groups and businesses to be better informed, involved and, where possible, empowered by undertaking self-service and digital interactions. This means we must make sure our citizens have trust and confidence in the way they can enter and access and the way we manage, store, share and use our information assets.

5. Responsibilities and Accountabilities

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

5.2 ***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. Compliance with Legal and Contractual Requirements

6.1 The Council has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation, mandatory compliance regimes and contractual requirements, including the:

- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Waste Electronic and Electronic Equipment Regulations
- Criminal Justice Secure Mail (CJSM) Service Terms and Conditions.
- Environmental Information Regulations 2004
- Protection of Freedoms 2012
- Human Rights Act 1998
- Public Services Network Compliance
- NHS Information Governance Compliance
- Payment Card Industry Compliance

6.2 If you are not sure of your responsibilities under any of these laws or mandatory compliance obligations contact the Council’s Information Governance Team for further information.

6.3 The Council’s Head of Governance & Assurance has specific responsibility for the Data Protection Act notification to the Office of the Information Commissioner.

7. Malware Protection

Everyone has a responsibility to make sure that the Council network and IT systems stay Malware free by complying with the Council’s Malware Prevention Policy.

8. Information Security Education and Awareness Training

8.1 All line managers must make sure that all persons that have authorised use of the Council's IT systems have adequate and appropriate training on:

- operating the technology and information systems provided
- completing required information security policy acceptance training as mandated by the Information Commissioners Office (ICO)
- understanding the security risks to their information systems
- using the security features provided within their information systems
- choosing, managing and protecting passwords and not passing them to others or leaving with their computer
- ensuring accounts are locked when absent from computers
- preventing the infection or spread of Malware and protecting data from the damage that Malware can cause
- identifying and protecting important, sensitive, personal or confidential data or records from loss, destruction and error
- applying agreed document classification and record retention schemes in accordance with best practice guidelines issued by relevant authorities
- only use Council supplied encrypted external storage devices
- ensuring the physical security of their desktop, laptop and other information assets
- identifying and reporting *security incidents.

An Information Security incident is an event that compromises the confidentiality, integrity or availability of information or information assets, having an adverse effect on security, reputation, performance or ability to meet regulatory or legal obligations

8.2 All line managers must make sure that employees are aware of procedures required for the management of non-electronic information:

- clear desk policy
- locking paper files away
- not leaving paper files unattended
- transport paper files securely and do not leave unattended

8.3 The Head of Governance & Assurance will continually review the level of awareness of Information Security within the Council and arrange awareness training when necessary.

It is a mandatory requirement from the Information Commissioners Office that all employees complete all aspects of Information Governance policy acceptance and training including Information Security via the Council's corporate E-learning tool.

9. Information Disposal

9.1 All information must be disposed of in accordance with the published Document Retention Schedule. Personal and sensitive information must be disposed of securely, for example, using a cross shredder or utilising the Council confidential waste disposal service. Please check with your manager about your confidential disposal process if you are unsure.

9.2 Obsolete equipment disposal must comply with the Council's disposal process which requires complete destruction of all data to the required standards set by government legislation. This includes storage devices containing confidential or personal data.

9.3 Software must be removed from computers and the media disposed of when the Software Licence Agreement expires. Software **must not** be used after the Licence Agreement has expired.

9.4 Remember to carry out regular housekeeping of business information in accordance with the Data Protection Act principles.

9.8 Mobile devices regularly used off site must have encryption software installed, this includes all portable media e.g. USB memory sticks. Computer devices used remotely must be regularly connected to the network for corporate update installations.

10. Incident Management

10.1 All security incidents **must be** reported using the form on iDerby and they will be investigated by the Information Governance team. See Appendix 1 for examples of security incidents.

10.2 It is the aim of the Council to capture and record all incidents so they can be managed successfully and lessons can be learned.

10.3 All incidents will be monitored and investigated if necessary and the Head of Governance & Assurance will report to Chief Officers, Line Managers and/or personnel as appropriate.

11. Business Continuity and Risk Management

The Council's critical business systems must be identified by the system and/or asset owners. They must ensure that a risk assessment is undertaken which will inform future resilience, service continuity and disaster recovery arrangements. This must be reviewed annually and submitted to the Information Governance team.

12. Compliance with the Information Security Policy

12.1 The Head of Governance & Assurance is responsible for monitoring compliance with this policy and will advise the Council's Senior Information Risk Officer (SIRO) and Chief Officers both periodically and following major incidents.

12.2 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.

13. Other Relevant Policies, Standards and Procedures

Network User Policy
E-mail and Internet User and Monitoring Policy
Data Protection Act Policy
Malware Prevention Policy
E-mail and Internet Monitoring Policy
Freedom of Information Act 2000 Policy
Document Retention Schedule
Serious Untoward Incident Reporting Policy
Criminal Justice Secure Mail service T&C's

The policy documents are on iDerby or contact the Information Governance team.

14. 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

Appendix 1

SECURITY INCIDENTS

An incident is defined as:

'An information security incident is an event that compromises the confidentiality, integrity or availability of the Council's information or information technology assets, having an adverse impact on the Council's, security, reputation, performance or ability to meet regulatory or legal obligations.'

Incident reporting involves a variety of differing situations and two categories are described below.

High level categories would include such things as:

- loss of personal, sensitive or business sensitive data in whatever format
- accidental disclosure of personal data
- loss or theft of a PC/laptop, information or paper documents
- loss of Confidentiality, Integrity or Availability
- system malfunctions
- loss of services, equipment or facilities
- degradation of the service
- access violations

Low level categories would include such things as:

- Malware infections
- password compromise
- misuse or abuse of the system
- backup failure and loss of data
- unauthorised access to premises or systems.

These lists are not comprehensive because, in reality, there may be a combination of any of the above categories.

If in doubt ask for advice and err on the side of security.