Derby City Council

Personnel Committee
14 January 2016

ITEM 8

Report of the Strategic Director of Governance

Malware Prevention Policy

SUMMARY

1.1 The report seeks to introduce a revised and updated policy that raises the awareness of all who have authorised access to Council computers of their responsibilities to minimise the risk of any malicious software (Malware) infections.

RECOMMENDATIONS

2.1 To reduce the number of Malware incidents infiltrating the Council Information Systems (IS).

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 an e-learning programme to ensure all accessing Council computers understand and act to minimise the risks of infections.

REASONS FOR RECOMMENDATIONS

3.1 A Malware incident could lead to a 'Denial of Service' that is designed to prevent legitimate users of a service from using that service. This could have financial implications if the Council was unable to fulfil its role.

3.2 The current policy was agreed in January 2010 and had outdated advice that referred to actions and methods that were no longer relevant after restrictions were put in place to limit staff actions on the IT network and equipment after December 2012.

3.3 There have been increasing occasions recently when users of the Council IS equipment have not recognised that their actions could introduce an infection. We need to have an effective policy that staff are aware of and adhere to as part of their working practices.

3.4 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.

SUPPORTING INFORMATION

4.1 The Department for Communities and Local Government guide from March 2015 'Understanding Local Cyber Resilience - A guide for local government on cyber threats and how to mitigate them' recommends that local governments produce policies that directly address the business processes (such as email, web browsing and removable media) that are vulnerable to Malware.

4.2 According to the East Midlands Council local authorities in the East Midlands have highlighted a notable increase in Spam and Malware recently.

OTHER OPTIONS CONSIDERED

5.1 We actively scan for Malware across our systems and protect all host and client machines with antivirus solutions that will actively scan for Malware. All information supplied to or from our systems is scanned for malicious content. New Malware is conceived constantly so all must be aware of actions they should undertake to help prevent infection.

5.2 Failure to issue an updated policy increases the risks which, should an infection 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: Malware Prevention Policy

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 There are no direct financial implications unless a ‘Denial of Service’ attack caused the Council to be unable to fulfil its role.

Legal

2.1 There are no direct legal implications.

2.2 The policy does highlight a certain level of responsibility is the individuals to follow the basic rules to keep a Malware infection to a minimum.

Personnel

3.1 The policy will apply to all staff with computer access. 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 Malware incident could lead to a ‘Denial of Service’ that is designed to prevent legitimate users of a service from using that service.

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.

Appendix 2

Organisation and Governance:
Malware Prevention Policy

Document owner	Richard Boneham, Head of Governance & Assurance
Document author and enquiry point	Angela Gregson
Date of document	October 2015
Version	6.0
Document classification	Official
Document distribution	Published via the Council intranet
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
November 2010	5.1	Issued	Update
October 2015	6.0	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

1.1 Malware is short for malicious software and covers viruses, worms, spyware, Trojan horses etc. Its various forms are designed to disrupt computer operation, gather information, corrupt and/or delete data on a computer and gain access to computers and networks. The most common way that Malware is spread is from an email attachment, downloaded internet file, infected CD/DVD or USB memory stick; they can infect networked and stand-alone computers.

1.2 This policy applies to all employees of the Council, elected members, contractors, agents, partners and temporary staff working for or on behalf of the Council. It applies to all who have authorised access to Council computers and have an email account and access to the Internet.

2. Policy Objective

2.1 The objective of this policy is to make users aware of their responsibilities and the things they should – or should not – do to minimise the risk of any Malware infections. It will raise awareness on:

- how they are introduced
- how to recognise an infection and/or a denial of service attack
- the consequences of an infection and/or a denial of service attack.

2.2 By understanding and implementing our responsibilities we will, minimise the risk of:

- an infection
- a denial of service attack

- data loss should Malware break through our defences.

3. Malware

3.1 Malware can be introduced to a computer by:

- downloading files from a web page
- launching software or tools from a web page
- infected web pages
- opening emails and email attachments from known and unknown external sources
- expanding compressed files sent by email (to avoid mail gateway security)
- CD’s and DVD’s
- external storage devices e.g. USB memory stick

3.2 The indicators of a possible infection include:

- applications that don't work properly
- file size changes for no apparent reason
- date of last access does not match date of last use
- an increase in the number of files on the system when nothing has been added
- unusual error messages
- system slows down, freezes or crashes

3.3 This list is not comprehensive but the consequences of a malware infection can include:

- lost productivity through data and devices being unavailable
- lost data and access
- legal implications if deadlines are missed
- financial loss if deadlines missed
- compliance failures which may mean partners or the government deny the Council access to their systems and data
- confidential and/or sensitive data being put into the public domain
- put at risk citizens or businesses whose data was compromised
- cost of additional compliance assessments to demonstrate security vulnerability has been closed
- cost of cleaning the network
- unreliable applications
- corrupted files

4. Hoaxes

4.1 Hoaxes usually take the form of an ‘urgent virus warning’ email message. They usually contain false reports about new undetectable viruses and urge recipients to forward the warning to as many people as possible. This mass forwarding then produces similar effects to a true malware infection and could potentially overload an email server. Another common hoax is when an email tells you to look for certain files on your computer and delete them and then email everyone in your address book. If you follow the instructions without checking if it is a hoax, you may delete essential system files which are necessary to run your computer.

4.2 Log a call with the [IT Service Desk]() if you suspect an email is a hoax for it to be investigated and they will notify [Information Governance]().

4.3 If necessary a malware warning will be issued by the Council's Head of Governance & Assurance or the [Information Governance team]() and an alert will be placed on iDerby.

5. Responsibilities and Accountabilities

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

5.2 Users must be aware that a certain level of responsibility is theirs and that this responsibility must be taken seriously.

5.3 Follow these basic rules to keep the risk of a malware infection to a minimum:

- if you have a Council mobile device it **must** be connected to the network ideally every week but at least once every 30 days so it can get the latest versions of malware software.
- never open an email attachment or a link in an email from an unknown external source
- do not reply or forward emails you suspect may be a malware attack or a hoax
- never download anything in response to a warning you get from a program you didn't install or don't recognize
- only download from reputable sites and then carry out a malware check on the file
- never connect a personal memory stick to a Council owned computer
- never leave any removable media in a computer when switching off
- never load software without authority to do so from the Information Systems department

5.4 Remember to:

- log any malware or suspected malware incident to the [IT Service Desk]()

5.5 If your computer becomes infected with malware:

- stop using the laptop/computer immediately and disconnect from the network
- report the infection to the IT Service Desk
- do not attempt to use the computer until it has been certified as infection free by an IT engineer.
- stop using CDs and DVDs

6. Our Defences

All computers are automatically updated daily with the DCC malware solution and users can click ‘Update’ in the console to ensure they have got the latest versions.

All emails that have zip file attachments (a type of compressed file that can be used to hide infections) will be blocked to protect the Council’s network. This is required due to recent attacks against the Council that used a zip file and to meet mandatory security regulations. Users will be sent an automated email from the email security system telling them when a zip file has been blocked.

7. Compliance with the Malware Prevention 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

Network User Policy
Information Security Policy
E-mail and Internet Monitoring Policy

The policy documents are 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