E-MAIL AND INTERNET USER POLICY FOR COUNCILLORS

DRAFT
Version 0.5

Document owner	
Document author and enquiry point	Alison Jones, IT Security Officer
Document authoriser	Mike Thompson, IT Manager
Date of document	September, 2002
Version	Draft 0.5(plain english)
Document classification	Internal
Document distribution	Internal
Document retention period	Until date of next review
Document review date	September, 2003

CONTENTS

1. Introduction and scope

The Council, provides access to Information Systems and IT facilities for business purposes. Employees and councillors 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, e-mail and Derbynet access are standard tools available to anyone provided with a computer that is 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 has to be or must not be done to specific requirements - mandatory.

3. Limited personal use

The Council allows reasonable incidental personal use of the e-mail and Internet to employees and councillors working on Council premises and linked to the Council network. Reasonable, incidental personal use by councillors working at home should be kept to a minimum as such use involves a direct cost to the Council.

4. Expectations

The Council expects you to use the e-mail, Internet, Derbynet and other technology responsibly at all times. Any alleged misuse of the e-mail system or Internet will be deemed to be a breach of the Council's Code of Conduct.

5. Monitoring

The Council reserve the right to monitor and log e-mail and Internet activity. This is generally required for quality control or identifying inappropriate use for training purposes. However, if we have evidence of misuse through monitoring it will be investigated thoroughly by the Council's monitoring officer.

6. Guidelines on acceptable use

Reasonable, personal use is allowed provided that it:

- does not damage the Council's interests
- does not involve sending or receiving any material that the Council considers offensive

- does not conflict with the Council's equalities or harassment policies
- is lawful under the **Protection from Harassment Act 1997,** the **Sex Discrimination Act 1975,** the **Disability Discrimination Act 1995** and the **Race Relations Act 1976,** the **Race Relations Amendment Act 2000** and the **Human Rights Act 1998**
- is not used to store, transmit or publish any material that is legally 'obscene' under the **Obscene Publications Act 1959**
- does not interrupt, disturb, inconvenience or degrade the service
- does not get in the way of the work of the Council
- does not break any of the conditions in section 7 of this policy.

7. Unacceptable e-mail and Internet use

You ***must not*** use e-mail and Internet for knowingly doing anything that is illegal under ***any*** law or for any of the purposes listed:

- promoting any commercial ventures, causes or organisations unless expressly authorised by the Council
- promoting any private or personal interests such as selling possessions or property or promoting a social activity not connected to the Council. We plan to make this facility available through Derbynet.
- taking part in activities, make statements, deliberately visit web sites or share or retrieve information or software containing material of a discriminatory nature, which would create an intimidatory working environment, based on ***sex, race, sexual orientation, age, disability, national origin or religion***
- sending messages or material using language or including images that are ***obscene, pornographic, sexually orientated, derogatory, offensive, threatening, insulting, harassing or harmful*** to recipients. The Council uses technology to detect and block unsuitable e-mail content.
- copying, distributing or receiving copyrighted or confidential material without the owner's consent
- describing techniques for criminal terrorist acts
- breaking through security controls, whether on Council equipment or on any other computer system – hacking
- deliberately accessing or transmitting a computer virus, worm, Trojan horse, trap-door program code or similar software
- knowingly do anything that could block or interrupt networks or systems, including sending chain or 'junk' e-mail
- deliberately hide your identity when sending e-mails or pretend to be someone else when using the Internet
- using e-mail to create or vary an existing contract on behalf of the Council
- downloading or running entertainment software or games
- knowingly downloading or distributing pirated software or data

This list is not comprehensive. Use it as a guide only. The Council will update it when necessary.

8. General conditions

E-mail

8.1 You should recognise that e-mail is not a secure way of exchanging information especially if it is private, confidential, personal or sensitive. Be aware of your responsibilities under the ***Data Protection Act 1998*** – DPA, and protect messages suitably. Use passwords to protect any documents. If you are not sure of your responsibilities under the DPA, or any other law, you will find further information on Derbynet under **Document Library/Policy & Strategy/Codes & Protocols**, in the Data Protection Act Councillor Guidelines or from your Information Services Manager.

8.2 Do not put anything into an e-mail, or an attachment, that you would not put on Council headed notepaper. E-mail can be used as evidence in criminal cases so be aware of how it would sound if read out in court. If in doubt, don't send it!

8.3 Recognise that the legal responsibility for defamation or false statements applies to e-mail. You must not knowingly make a libellous or false statement about any individual in e-mail as you personally **and/or** the Council could be held responsible and liable for any damage it causes to the reputation of the victim.

8.4 To avoid introducing viruses into the Council's network, do not open e-mail attachments from unknown external sources.

8.5 Only Departmental IT liaison officers may send 'All User' e-mails. If you want to send an all user e-mail, please contact your Information Services Manager. See Appendix 1 for contact details.

8.6 Keep e-mail and Internet passwords secure. Do not reveal or share them with anyone. Set suitable permissions within your mailbox if you require other people to have access to your mail. If you need help contact your Information Services Manager.

8.7 It is a criminal offence under the ***Computer Misuse Act 1990*** to access a computer system without authority to do so. Do not read, delete, copy or change the contents of anyone else's mailbox without their permission. This includes when someone is unexpectedly away from the office.

8.8 If you have a password protected screensaver function, use it.

8.9 All external e-mails have a disclaimer message automatically attached - see Appendix 2 for disclaimer detail.

8.10 External e-mail messages must always contain your name and contact details - see Appendix 3 for the Council standard format.

Internet

8.11 Only subscribe to bulletin boards, newsgroups or any other Internet Service if you need to as part of your council duties but please be aware that they are public forums so you must not reveal any confidential Council or service user information.

8.12 Always disconnect your Internet access when not in use. Always log off or use a password-protected screensaver if you need to leave your PC unattended for any length of time.

8.13 If councillors use the Internet to buy goods or services the Council will not accept liability for default of payment or for the security of any personal information you give, for example credit or debit card details.

Derbynet – the Council's Intranet

We encourage councillors to make use of Derbynet, to view Council information.

9. Virus protection

Everyone has a responsibility to make sure that the Council network and IT systems stay virus free by complying with the Council's Anti Virus Policy. A copy of the policy is on Derbynet under **Document Library/Policy & Strategy/Codes & Protocols** or contact the IT Security Officer.

In summary:

- never open e-mail attachments from an unknown external source
- check all diskettes for viruses before use
- make sure you have the latest version of the Councils anti-virus software -guidelines on how to do this are at Appendix 4
- always report incidents on virus detection to your Information Services Manager.

10. Other relevant policies, standards and procedures

Information Security Policy
Data Protection Act Policy
Anti-virus Policy
Data Protection Act Councillor Guidelines Leaflet

All these documents are on Derbynet under **Document Library/Policy & Strategy/Codes & Protocols** or contact the Council's IT Security Officer.

11. Contact details

Please contact your Information Services Manager, the Council's IT Security Officer or anyone in the Central IT Unit team with enquires about this policy or any other referenced policy, procedure or Law - see Appendix 1 for contact numbers.

12. Document version control

The current version of this Policy will always be available on Derbynet. Please check version control either on the Intranet or with the IT Security Officer when using printed copies.

Date Issued	Version	Status	Reason for change
Sept 2002	0.1	Draft	
15 Oct 2002	0.2	Draft	SVG & CL Comments
18 Oct 2002	0.3	Draft	SD Comments
28 Oct 2002	0.4	Draft	Location details
26 Nov 2002	0.5	Draft	Points of detail

13. Appendicies

- appendix 1 – Contact numbers
- appendix 2 – E-mail disclaimer details
- appendix 3 – Council standard e-mail formats
- appendix 4 – Guidelines on how to upgrade Anti-Virus Software
- appendix 5 - E-mail good user guide

14. Terminology

Term	Definition
Hacking	The term given to someone who tries to gain unauthorised access to a computer system in order to steal or corrupt data
Trap-door program code	A trap-door is a code that allows a programmer to gain access to a secure computer system at some later date – it is also known as back door program code
Trojan Horse	A destructive program that pretends to be a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive. One of the most dangerous types of Trojan horse is a

	program that claims to rid your computer of viruses but instead introduces viruses on to your computer
Virus	A program designed to replicate and spread on its own, preferably without a user's knowledge. The spread by attaching themselves to another program, such as word processing or spreadsheet programs, or the boot sector of a diskette. A more dangerous type of virus is one capable of transmitting itself across a network and bypassing security systems – see Worm
Worm	A program that spreads itself over a network, duplicating itself as it goes

Appendix 1

CONTACTS

Information Services	Colin Lawrence	25 5590
	Lee Haynes	25 5558
Central IT Unit	Mike Thompson ***IT Manager***	25 5565
	David Gale ***Business Analyst***	25 6260
	Terry Tinsley ***IT Contracts Officer***	25 6204
	Alison Jones ***IT Security Officer***	25 6262
	Helena Rooms ***Systems Developer***	

Appendix 2

DERBY CITY COUNCIL E-MAIL DISCLAIMER

****
The views expressed in this e-mail are personal and may not necessarily reflect those of Derby City Council, unless explicitly stated otherwise.

This e-mail, and any files transmitted with it, are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error, please notify me immediately.

If you are not the intended recipient of this e-mail, you should not copy it for any purpose, or disclose its contents to any other person.

This footnote also confirms that this e-mail message has been swept by MIMEsweeper for the presence for computer viruses. However, we cannot accept liability for viruses that may be in this e-mail. We recommend that you check all e-mails with an appropriate virus scanner.
****

Appendix 3

DERBY CITY COUNCIL STANDARD E-MAIL ADDRESS FORMAT

firstname.lastname@derby.gov.uk

In exceptional circumstances when there may be two or more employees with the same name, a number may be included following the last name.

firstname.lastname1@derby.gov.uk

Use this format when using the 'signature' facility on Outlook:

Name	**Councillor A N Other**
Derby City Council	**Derby City council**
e-mail	**ann.other@derby.gov.uk**
Tel +44 (0) 1332 tel number	**Tel: +44 (0) 1332 256262**
Fax +44 (0) 1332 fax number	**Fax: +44 (0) 1332 256267**

Appendix 4

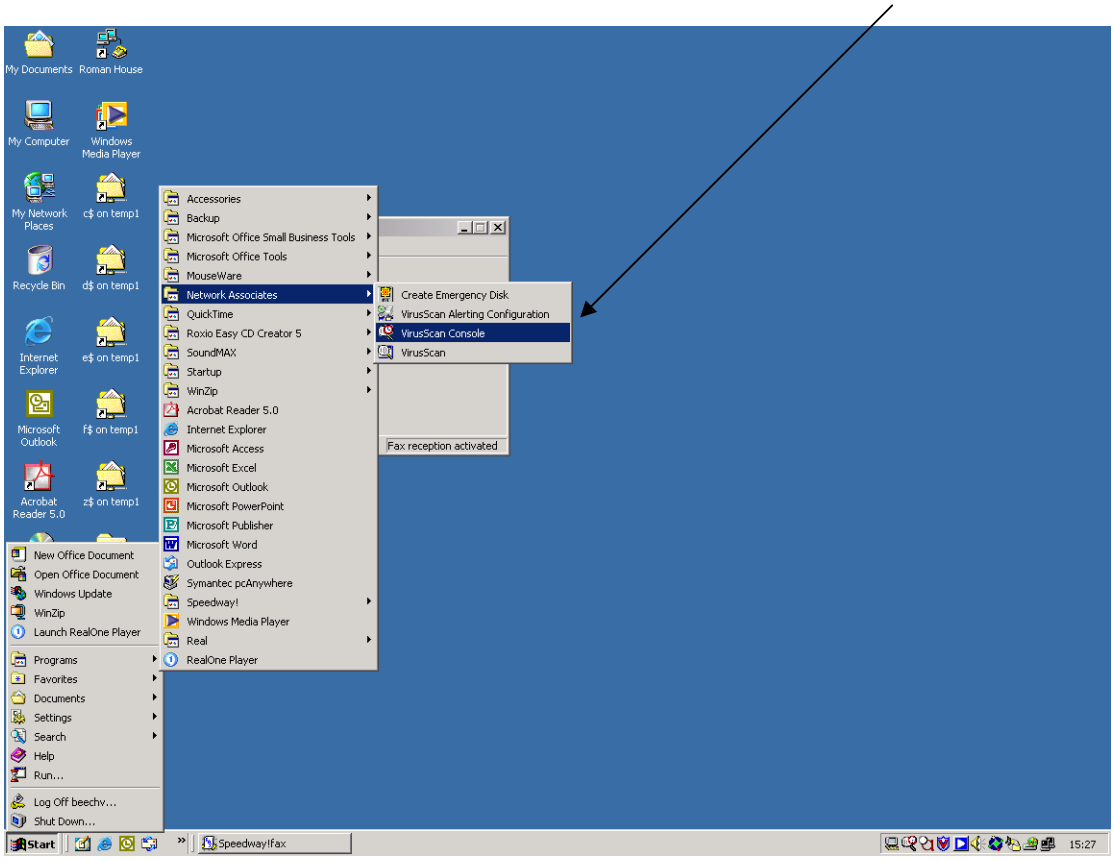
GUIDELINES ON HOW TO UPGRADE ANTI-VIRUS SOFTWARE

Please make sure Microsoft Outlook is **NOT** running and close any other programs

1. Connect to Roman House

2. Start the VirusScan Console – like this

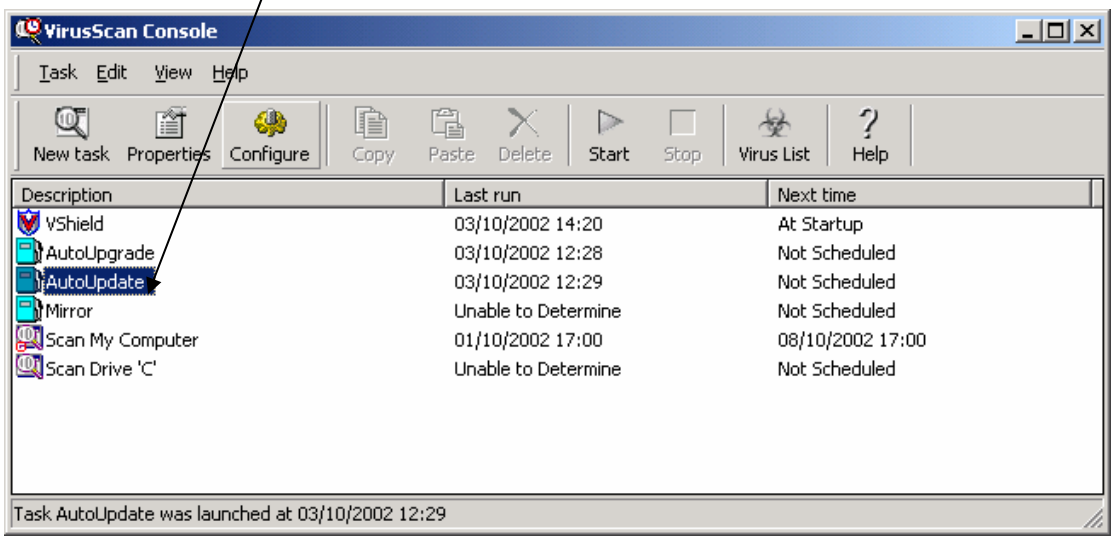
Click **Start**, **Programs**, **Network Associates**, **VirusScan Console**



Then wait – maybe as much as 15 seconds for it to load.

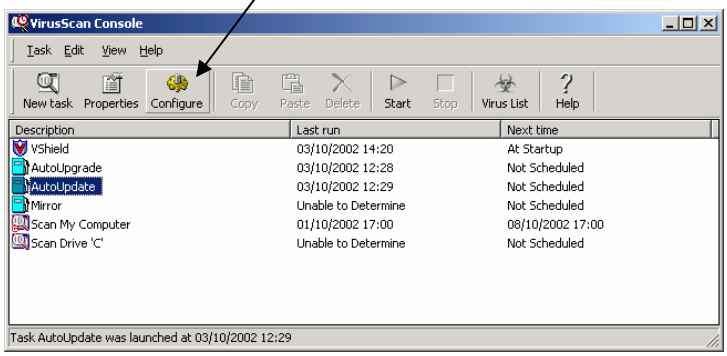
You should now see a screen like the one shown below.

Please click once on **AutoUpdate**



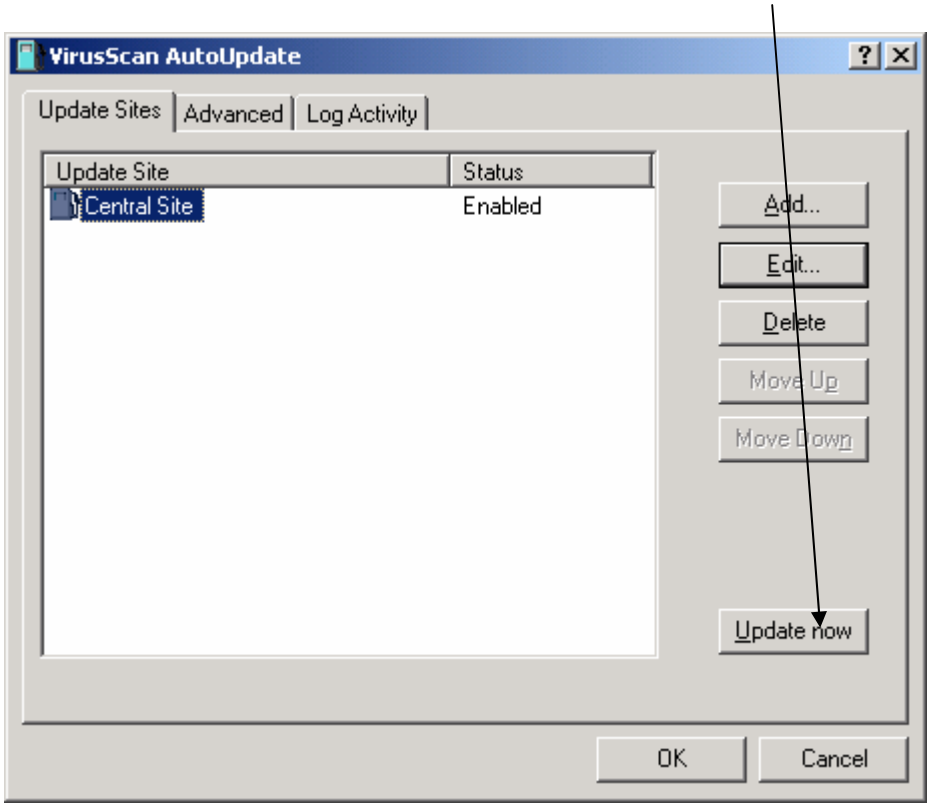
3. Tell the software where the update file is located.

Click on the Configure Button.

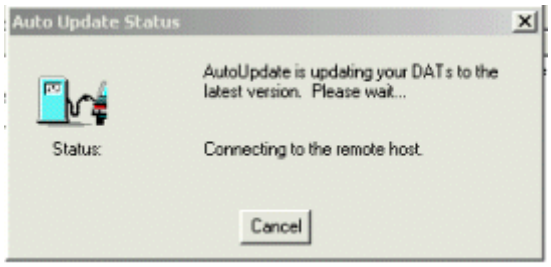


4. Next step do the update

You should now see a screen like this Click on the **Update Now** button



You should now see a smaller “progress” box, similar to the one shown below. Please wait whilst the file is fetched from the software manufacturer’s site –



this may take up to 10 minutes.

The information in the progress box will change from time to time to inform you how far it has got in the process. When it has completed, it will read so and the cancel Button will Change to **OK**.

Click **OK**, then you will be returned to the VirusScan Console Screen.

Close VirusScan Console using the ☒ on the top right hand corner.

5. Final Step - Please Disconnect from Roman House

Appendix 5

E-MAIL GOOD USER GUIDE

Do:

- maintain your mailbox correctly:
  - open e-mails at least once a day
  - set your 'out of office' message if you are going to be out of the office for longer than 1 day
  - set permissions for others to see your mailbox if you want them to have access
  - clear your 'Deleted Items' folder daily

- use a password protected screen saver to avoid unauthorised access to your PC or e-mail
- make sure you are aware of the sensitivity of e-mail contents or attachments before sending. An unrestricted or unclassified e-mail message can disguise a highly sensitive attachment. **Always** use password protection for sensitive documents.
- make sure the 'subject' field holds a meaningful title
- develop orderly filing systems for messages you need to keep
- keep messages brief and to the point. Some people find it harder to read from the screen than from paper.
- make sure you are sending your message to the correct person

Don't :

- print out e-mails unless you really need to
- send a message in capital letters. It is the electronic version of **shouting**!

- assume the message has been received or read just because it has been sent

- reproduce the message sent to you unless it is really necessary

- send large attachments – this can slow down or even stop the e-mail system

Remember:

- your responsibilities when using e-mail and the Internet

- the Council reserves the right to monitor e-mail and Internet activity

- never share passwords

- it is an offence under the **Computer Misuse Act** to access someone else's mailbox without their permission

- your responsibilities under the **Data Protection Act** and never disclose personal or sensitive information in an e-mail message

- never open an e-mail attachment from an unknown external source

- always add your contact details to external e-mail messages

- don't send out 'All User' messages. Contact your Information Services Manager to do it for you.

- e-mails already have a disclaimer message attached when sending externally so you don't have to add your own

- even experienced e-mail users make mistakes so always check that the e-mail you are about to send:

  - communicates the intended message
  - has the appropriate tone
  - is addressed only to the correct recipients
  - has had the spelling checked.

- it is your responsibility to check the sensitivity of the message or the attachment. Always check before sending . . .

  - is the message sensitive?
  - is the attachment sensitive?

- am I sending it to one person or a list of recipients? If a list is everyone on the list entitled to see the message? Do I want them all to see the message?
- if the message is too sensitive, should I be using e-mail at all? Consider a controlled fax message or telephone call, followed by normal mail.

- always be careful when forwarding e-mails – particularly if you don't want the original writer, or someone else on the circulation list, to see your comments. Clicking on the 'reply to all' option could reveal confidential or embarrassing information to Council employees, other councillors, clients or suppliers. Remember to:

  - double check where your mail is going
  - read every recipient's name before you send it
  - when everything is checked and you are sure it is correct, then send the message. If in doubt, don't send it!

- If in doubt about anything, ask. Contact the IT Security Officer.