

This factsheet will help your business develop and establish an appropriate e-mail policy.

CONTENTS

INTRODUCTION

HINTS AND TIPS

CASE STUDIES

CHECKLIST

GENERAL BUSINESS ADVICE

INTRODUCTION

With regard to personal e-mail, the only yardstick that you can use to measure reasonableness is common sense. Such an approach is difficult to police consistently, for example:

- Employee receives a joke via an external e-mail from a friend
- Employee forwards the joke to a colleague via internal e-mail
- That employee forwards the joke to an internal distribution list
- Another employee forwards the joke to a friend externally
- The joke is sexist/racist

Your company could be held liable for any offence caused by the joke.

This factsheet is for any business trying to introduce an e-mail policy. It covers hints and tips for implementation and case studies illustrating how e-mail problems can multiply.

HINTS AND TIPS FOR EMAIL POLICY

The following points may be relevant when considering inappropriate usage. You may wish to consider them whilst establishing your own e-mail policy. The list is by no means exhaustive, but might provide at least a good starting point.

E-mail

- Minimise the forwarding of e-mails that contain non-business material
- Check receipt of important messages with a telephone call
- Never divulge your password or account information to other users
- Be aware that the sarcasm, humour, abuse, or tone can easily be misunderstood in e-mails
- Avoid using currency punctuation in text-based e-mails. Use three-letter currency indicators instead (e.g. GBP, USD, EUR)
- If possible, refer to files on any network-shared areas rather than include the files as an attachment
- Send e-mails to individuals rather than groups
- Compress large attachments, if possible, before sending, for example, zip files
- Ignore and delete chain e-mails
- Avoid subscription services and automatic information services unless there is a good business reason for subscribing
- Check the authenticity (for example, by telephone) of suspicious messages
- Carry out regular housekeeping on your mailbox. Delete all e-mails as soon as possible and ensure that there is only one copy of any attachment in your mailbox
- Keep the number of e-mails in your mailbox to a minimum
- Check your personal address book regularly and remove unwanted and incorrect entries
- Always check that the addressee names are correct and be particularly aware of personal or global address groups

Sending Emails from the Internet

- There are no guarantees of delivery
- Mail may be delivered to the wrong person
- The message may not be delivered in its original format, i.e. it can be modified
- Mail received may not be from the apparent source; i.e. it can easily be spoofed
- Mail can be read or copied by others

Security Passwords

- Always log out of systems when they're not in use
- Never leave an e-mail account unattended if it is logged in unless a password protected screen saver is invoked
- Do not log onto an e-mail account other than your own, even if requested to do so
- Do not send e-mail messages from another user's mailbox
- Keep your password confidential. Never divulge it to anyone and never enter passwords when others can observe your keystrokes
- If you suspect that others know your password, change it immediately

CASE STUDIES OF INAPPROPRIATE USE OF EMAIL

The Organisations

Some of the firms involved in the cases below are quite large, but the implications of the following case studies can relate to any company, irrespective of size or industry.

What happened

Event 1

A lawyer at a City of London firm sent an e-mail telling friends about his girlfriend's sexual tastes. The e-mail was circulated to a small group of friends but within a week the message had been distributed to over a million people. Within two weeks, it had spanned the globe.

Event 2

A UK mobile telephone company sacked up to forty staff for downloading pornographic images from the Internet, using company systems and company time.

Event 3

A city banker wrote an e-mail describing his sexual exploits. One of the five original recipients forwarded the e-mail, and many of those who received it did the same. Hundreds of thousands of people were sent the offending article, including employees at:

Bank of England

Barclays

HSBC

Daily Telegraph

Capital Management Group

KPMG

Impact

Few of these events would have had a direct financial impact on the companies involved, but there can be significant losses due to consequential and subsequent events. These events include:

- PR management of the consequences
- Wasted staff time dealing with enquiries
- Wasted system resources, including disc space and bandwidth

Lessons

Given the conversational nature of e-mail, it is almost inevitable that people use it (including work e-mail) for every purpose. Many companies tolerate reasonable personal usage, as to ban it would be impractical, and have potential legal implications. To manage this circumstance, it is essential that you:

- Inform your staff what is and is not acceptable
- Make sure everyone knows that there are

circumstances when you will monitor e-mail traffic

CHECKLIST

Risk

Any organisation, irrespective of size, can take a few basic steps to minimise the risks from inappropriate usage. Do you have the following?

- Appropriately configured virus defence software
- A facility for checking, quarantining and managing e-mail attached files
- A way of checking who has accessed what site on the Internet
- A legal disclaimer automatically attached to outgoing e-mails
- A clear and unambiguous policy on e-mail and Internet use
- A means of communicating your policy to those who need it
- Awareness of legal implications for monitoring staff activity. This is a thorny issue that needs careful management

Recovery

The following high-level principles should be considered before setting up a formal response to an incident:

- The best aid to recovery is prevention
- Make sure those involved understand their roles and responsibilities. Ensure that people know who's in charge and has authority to speak for the company
- Clarify channels of communication to all who need to know, including external parties such as the media
- Make sure those interested know what you have done in terms of preparation. This should include a published policy, education initiatives, warnings and other pre-incident activities

- The media can be your friend as well as your enemy; make them your friend
- Remember that failing to disclose information to the media can rebound on you if they find it out through other channels; make use of any PR people you employ
- Remember that the aim is to manage the effects of the incident. Don't be tempted to use 'spin' as an alternative; it will rebound on you

Prevention

- Ensure that you have policies regarding the use of e-mail and the Internet
- Ensure that your policies state clearly what is and is not acceptable use
- Ensure that virus defence software is installed and that it is configured appropriately for your systems
- If necessary, consider the use of content filters to prevent access to websites that are considered unsuitable
- If you are considering monitoring staff usage of e-mail and/or the Internet, make sure that you stay within the law if in doubt, seek professional advice

GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business: Contact your local Business Link advisor by visiting the website at <http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and Industry. <http://www.dti.gov.uk> © Crown Copyright