An email policy for your employees

Most businesses use email as a key communication tool. It can be a quick, convenient and effective way of contacting both customers and other members of your team, without the disruptive effect of a phone call.

But if you use email or plan to introduce it, you need to set up a clear email policy. This will help you prevent timewasting, protect the security of your systems and data and minimise the risk of legal problems.

This briefing outlines:

- The key elements you need to include in your email policy.
- How to implement and enforce the policy.

1 Permitted use

1.1 In an ideal world, employees would only use company email systems for **business** purposes. In reality however, this is unlikely.

- You cannot stop employees receiving personal emails.
- Allowing some personal use of email may improve your employees' morale, and even efficiency.

1.2 Limit personal use.

You might prohibit:

- Excessive personal use of email.
- Inappropriate or illegal content (see **2.3**). Offensive jokes can be a particular problem.
- Engaging in illegal activities. For example, using email to harass someone or deliberately sending a virus.
- Encrypting personal emails and attachments.
- Running a personal business while at work.

Consider giving employees separate personal addresses. Emails can then be filtered into separate business and personal folders.

1.3 Set out **when** email should and should not be used (see **3**).

2 Content

2.1 Make employees aware of the **style** and tone you expect them to use.

This is usually somewhere between the informality of a telephone conversation and the formality of a letter.

- As a rule of thumb, you should adopt the same style as your contacts.

An overly formal style may seem laboured and tedious to people used to quick, friendly emails.
- Some industries, and some nationalities, have their own standards.
- Short emails can appear brusque.
- Typing in capitals is the email equivalent of shouting, and can be considered rude.
- Use a formal letter style for formal documents or when approaching someone for the first time.

2.2 Set up your software's signature feature to add **letterhead** details, and any disclaimer, to your messages automatically.

- If possible, get it to attach alternative details to personal emails.

2.3 Specify what content is **prohibited**. This should include:

- Sexist, racist or other offensive material.
- Defamatory material.
- Content which is protected by copyright.
- Links to inappropriate material.

Instant or not

Your employees need to be aware of how quickly an email will be transmitted in order to judge whether it is the most suitable option.

A If you, or the recipient, only have **dial-up** Internet access, emails will be a slow method of communication.

- Emails will only be sent and received when you and the recipient connect to the Internet, although internal emails will be transmitted immediately.
- You can dial-up specifically to send or check for urgent mail.
- If an email is urgent, you may want to telephone once you have sent it.

B Most businesses now use a broadband connection. Recent Ofcom statistics also show that over half of all UK households now have a broadband connection (Ofcom International Communications Market report 2007).

- A broadband connection enables emails to be sent and received almost immediately as the connection is 'always-on'.

3 Sending emails

3.1 Employees should use their own, password-protected **accounts** to send emails.

- Passwords should be strictly controlled.

3.2 Encourage the use of emails, rather than phone calls for communications you wish to keep a **record** of.

3.3 Get employees to use emails for **internal communications**.

- Unlike a phone call, email can be dealt with at the recipient's convenience.
  But beware of allowing internal email to become excessive (see **3.7**).

3.4 Establish **standards** for outgoing messages.

- Set out what typeface, type size and colour should be used.
- Consider putting a limit on the size of any attachments.
  Many Internet service providers place restrictions on attachment size (eg 5Mb).

3.5 Have rules for handling **confidential** information.

- You may want to ban certain types of information from being sent by email.
  For example, lists of customers and information about new products.
- You might specify that some information can only be sent using encrypted email.

3.6 Explain the potential **contractual** significance of emails to employees.

An email can be as contractually binding as any other form of communication.

- You may choose not to use email for any contractually significant communications, and insist that all such documents are sent by letter instead.
- Consider including a disclaimer on emails.
  For example, an extremely simple disclaimer might state:
  'This email is confidential, and is intended for the use of the named recipient only. If you have received this message in error, please inform us immediately, and then delete it. Unless it specifically states otherwise, this email does not form part of a contract.'

3.7 Sending too many emails can lead to **information overload**.

Excessive email, particularly internally, can

"Once you've set up your policy, make sure you revise it regularly to reflect any changes in the law, or in the way your business uses email."
Steve Newton, Galatea Training Services

lead to overwork or a tendency to disregard emails. It can also seem rather impersonal.

- If you send and receive a large amount of email, it becomes far easier for an important message to go unnoticed. Consider adding 'priority flags' to emails to indicate what is and isn't important.
- Avoid sending emails when you would not have sent a letter or memo, or made a telephone call, if email was not available.
- Before sending a message to a large number of people, ask yourself whether they all really need to receive the message.
- Replying to all the other recipients of an email you have received, as well as the sender, is another common problem. Some companies ban use of the reply-to-all feature completely.

Avoiding viruses

Attachments can present particular problems, as they may contain potentially harmful viruses.

If you have a central mail server equipped with up-to-date anti-virus software, the risks will be far lower than if you have dial-up access. But as recent cases have shown, such protection is not always enough.

Make a procedure for dealing with attachments part of your email policy.

A **Delete** attachments from unknown senders, unless you expect to receive such files from new contacts as part of your job.

- Empty the deleted emails folder.

B Take care with certain **file types**.

- Some kinds of file are more likely to carry viruses.
  For example, file names including .vbs, .js, .exe, .bat, .cmd or .lnk extensions.
- Compressed files (containing .zip, .arc or .cab) may also contain such file types.

C Get **advice** from the IT manager if you are unsure.

- Always inform the IT manager if you receive a suspicious attachment or if you suspect a virus has entered the system.

  Get your IT manager to keep up to date with new viruses and warn all employees about them when necessary.

- If you have an intranet, cut down on internal emails by posting messages on your intranet instead.

3.8 Explain your policy on **storing** both sent and received emails.

- Your system may be set up to handle email filing automatically.
- Some companies print out paper copies of important emails to be filed with other documents.
- Stored emails need to be protected from any later editing or unauthorised deletion.
- Back up all email data regularly as part of your normal back-up procedure.
- Inform employees about the permanence of emails. For example, if emails are stored centrally even after employees have deleted them from their own accounts, make them aware of this.
- You must tell employees how emails are monitored (see **6**).

4 Receiving emails

4.1 Set out **who should read** incoming emails.

- Generally, employees should read only their own emails (using their own passwords to access the system).
- Establish how you will handle emails sent to a general address you might have (eg info@company.co.uk).
  Assign responsibility for dealing with such emails and set up your technology so that only the relevant people can read them.
- The policy should also cover how incoming emails are handled when employees are absent (eg on holiday). (See **5.4**.)

4.2 Set out your **security** procedures for dealing with viruses.

- Employees should follow the procedure for dealing with attachments (see box on p3).

4.3 Set a **response** time.

- You might stipulate that all incoming emails should be replied to, or at least acknowledged, within 24 hours.
  Depending on your industry, a faster response time may be more appropriate.
- Software can help you filter and prioritise emails.

4.4 Explain how emails should be handled when an employee is **absent or leaves**.

- A simple option is to use an auto-

responder saying that the employee has left or how long the employee will be absent, and giving an alternative contact.
- If you choose a system where someone else checks the employee's emails, explain how personal emails will be handled.

4.5 Explain how **unwelcome** emails should be dealt with. For example:

- Ask employees to tell friends not to send them inappropriate emails.
- Delete junk emails (spam).
  It is not usually a good idea to respond to spam, even just to ask to be taken off a mailing list. A response confirms that the email has been sent to a live address.

4.6 Set out your policy on **storing** incoming emails (see **3.8**).

5 Monitoring email

There are legal restrictions on how you can monitor employees' use of email, although this remains a grey area.

You must use your policy to inform employees about how you will monitor emails, and for what purposes. You should include a clause on email monitoring in your employment contracts. If you fail to do so, you will need to get consent if you want to perform checks.

5.1 Tell employees how email **traffic** is monitored.

- If you use monitoring software to produce a log of sent and received emails, you should make employees aware of this.

5.2 Explain that you reserve the right to read **individual emails**.

You may inspect individual emails for 'specific business purposes', including:

- Establishing the specific content of transactions and other important business communications.
- Making sure employees are complying both with the law and with your internal policies.
- Preventing abuse of your telecoms system.
- Checking emails when employees are on leave.

If you wish to make interceptions for other purposes (eg marketing), you will need the consent of the sender and the recipient.

6 Implementation

6.1 Consult employees on what you should include in your email policy.

6.2 Consider taking **expert advice**.

- Although many aspects of your email policy will follow standard guidelines, it may be worth consulting a solicitor or other adviser.

6.3 Make the policy **available** to everyone.

- Ask employees to sign a copy to confirm they have read it.
- Refer to the policy in your employment contracts.
- Make sure managers familiarise themselves with the contents of the policy.
  Provide a contact name for employees who have any questions.

6.4 Put in place any **software** that will help. This might include:

- Monitoring software to provide a record of email traffic.
- Filtering software to help employees prioritise emails.
- Auto-responder software to reply to emails when employees are absent.
- Virus-checking and other security software.

6.5 Provide any **training** that is needed.

- Employees may need training in effective use of email software.

6.6 Enforce the policy.

- Make an individual responsible for enforcing the policy.
  Typically, the network administrator will be responsible for routine enforcement.
  A director should take overall responsibility.
- Apply the policy consistently and fairly to everyone, including yourself.
  Clarify any exceptions.
- Make sure you have an appropriate disciplinary procedure in place to deal with breaches of the policy.
- Revise the policy when necessary.

The policy will only provide legal protection if it is properly implemented and enforced.

Expert contributors

Thanks to **Richard Baker** (Sequence, www.sequence.co.uk, 029 2025 2555); **Steve Newton** (Galatea Training Services, www.galatea.co.uk, 01706 351389).

Published by BHP Information Solutions Ltd, Althorp House, 4-6 Althorp Road, London SW17 7ED
Tel: 020 8672 6844, www.bhpinfosolutions.co.uk