

## EMAIL: KILL OR KEEP?

*Different rulings have created confusion about email management. John Hookham (pictured) looks at the issues and the different approaches available.*



Over the last decade the internet has moved from being a closed tool for the university boffins to become ubiquitous. Email and the world wide web are available to the masses and for many organisations digital media is now the preferred method of communication.

However, the web was initially seen by many as the new electronic 'wild west'; governments and lawyers had no jurisdiction; you could say and publish anything you wanted on a website; you could send scurrilous emails; and you could not be sued or even be identified.

Today, we have an information-based economy, and email has evolved to become the preferred method of communication for business and increasingly for personal use. Most companies no longer have a post room or individually named racks of trays to receive the incoming mail. If you do receive a 'real' letter, it will probably be given to you directly by reception and become a talking point during the coffee break.

But in this brave new world of email and Google, some old-fashioned views about the free-for-all electronic wild west still linger in phrases such as 'it's only an email', 'an email is not a contract...it's not legal or anything' or 'I know I shouldn't have sent that email, but it's OK, I've deleted it'.

### Personal email

The vast majority of companies cannot function without IT and specifically email, which is now used to process over 80% of all business transactions. Email has become a key focus area for the IT function, with the number one concern being security and ensuring software viruses are kept off the network.

Not surprisingly, Forrester Research found in a recent survey of 1,000 companies that 33% were actively monitoring email and not just for viruses. Overall, 50% of respondents were concerned about email content and in particular the content of attachments.

Monitoring both incoming and outgoing email could be seen as the right thing to do, helping to protect the company and its business. However, when looking at email traffic, IDC Research found that up to 40% of emails were unconnected with company business – ie, they could be viewed as being private and personal. Monitoring or looking at these private emails could contravene the Data Protection Act, which is there to safeguard an individual's rights to privacy, even when using the company's business tools, such as email.

The solution would seem to be to delete all personal emails after they have served their purpose. This would comply with the Data Protection Act, which states that 'data can be kept for the purpose and for no longer than necessary for the purpose to be met'.

Clearly this approach is fine for internal emails to colleagues relating to, for example, 'sofa bed for sale' or 'the charity run is on Saturday, please sponsor me'. But emails may not always have an easily definable time period or validity. They could contain information relating to defamation of character or discrimination due to race, sex, religion, etc, in which case the emails may be needed as evidence as part of a court case at some time in the future.

It is also common practice for the HR department to use email when people join, leave or have assessments and for communicating health & safety information, and these types of email could contain both personal and business information.

So the answer would seem to be to keep all emails that contain personal information indefinitely – because how long is 'no longer than necessary'? This appears to be supported by the Financial Services and Market Act 2000 which states that when conducting a review 'a person has a right of access at any reasonable time to all such documents as may be reasonably required for the purpose of the review'.

The conundrum is: do you keep personal email indefinitely to avoid falling foul of the Financial Services and Market Act, or delete all personal email as soon as possible to comply with the Data Protection Act?

As more legislation gets passed, we have increasingly moved towards a 'blame and sue' culture, especially for loss of employment. Previously, cases of unfair dismissal or redundancy often cited TUPE (Transfer of Undertakings Protection of Employment) legislation as grounds for compensation. But increasingly, cases of unfair dismissal are using email as evidence and often the claim against the company has changed from TUPE, to that of discrimination or harassment. Normally settlements for unfair dismissal are capped at around £56,000, but for cases involving discrimination or harassment there is no cap and companies could be liable for compensation payments of £1 million or more.

Of course, as with all legal cases there still needs to be evidence that supports the claim. For example, in one case a female employee who had been sent 1,500 emails related to her private life during a six-month period claimed sexual harassment; but she lost the case as other emails showed that she had also sent joke emails of a sexual nature to other colleagues.

For business transactions, the Limitation Act states that the documentation needs to be retained for six years after a contact has been completed or fulfilled. However documentation may remain relevant (and need to be retained) long after the statutory six-year period has expired – such as in the case of asbestos-related illness where claims go back to incidents that happened 20 or even 30 years ago.

### **Email as evidence**

If an individual or company shreds printed documents which could be viewed as evidence in a court case then an additional offence has been committed, namely contempt of court. This has serious implications for both the individual and the company. The individual could be jailed and the company's case could be struck off.

Information that is stored electronically such as email has the same status as printed evidence; equally, data on a computer's hard disk is also admissible as evidence. Deleting email or not taking sufficient steps to retain email and electronic data can also be contempt of court. For example, Samsung had to pay legal costs of \$500,000 when it could not produce emails that were relevant to a court case.

There is one other major disadvantage with deleting email – the recipient or sender of the email will have their own copy and they could also have 'forwarded' copies to other people both inside and outside the organisation.

### **Burden of proof**

Phishing emails asking you to confirm your personal details to a unfamiliar bank are all too common, and are easy to identify as being fraudulent. There is a perception that the burden of proof for electronic documents is different to that required for



typed and signed letters, contracts, etc.

In the case of *Stouffer v Rowling*, evidence in the form of a printer's proof from 1987 was submitted by Stouffer as evidence that she had first used the term 'Muddles' in the book about her character Larry [sic] Potter. But an expert verified that the printed document used a font that was not invented until 1993 and was clearly forged or modified at a much later date. With email evidence, it may be necessary to use software experts to verify the originality of the email and verify that it has not been changed.

## E-signatures

In 1667 a law was passed in England that that still has repercussions around the world today. This stated that to be valid, any contract had to have a signature. Many people still believe that contracts (or changes to an employment contract, for example ) are not valid without a physical signature signed in black or blue ink.

In the case of *Hall v Cognos*, the company had a policy of not paying any expenses submitted more than six months after they were incurred. Mr Hall not only claimed expenses that were more than six months old, he also inflated the claim and was dismissed. The company refused to pay any part of the expense claim. However Hall's line manager had previously indicated in an email exchange that the expenses would be paid even though they were being submitted late.

The company argued that the email was not a valid variation of contract and was not binding on the company because all changes to contracts (in this case allowing submission of expenses that were more than six months old) had to be in writing. The judge ruled that the line manager together with the HR person who had sent the email had the authority to enter into the commitment on behalf of the company. The email formed a valid contact between Mr Hall and the company, and Mr Hall was entitled to the incurred expenses.

## The way forward

One major obstacle to email management has been overcome during the last few years. Disk storage used to be a major issue. Typically users were given a disk quota, often just an arbitrary figure, and were told to delete old files if they ran out of space. Today disk space is cheap and so every message and attachment can be retained.

This, coupled with new legislation, has allowed the IT department to switch its focus from disk storage monitoring to providing a comprehensive email management system – the first step being a clear written policy on personal emails; how long they will be stored for, and if they need to be looked at, under what circumstances and by whom, etc.

Email is by its very nature unstructured and is in many ways like normal everyday conversation, covering and referencing a number of different and often unrelated topics.

To meet the need for effective and efficient email archiving and management, a number of companies have produced software solutions. Legislation is constantly changing and its complexity will only increase – so rather than look to an inhouse solution, a specialist application looks to be the best option. For example, after an extensive evaluation, law firm Mills and Reeve adopted the Zantaz Enterprise Archive Solution. Cryoserver has a solution that works with all the major email systems such as Microsoft Exchange and Lotus Notes. This requirement is also being addressed by the ERP solution providers such as Lawson, SAP and Oracle.

The real decision is not whether you need to address email archiving and its management with a compliant policy – the legal requirement, if not overwhelming today, will be mandatory in the future. But do you choose a 'best of breed' option today and have full compliance – or do you implement an interim solution and wait for the integrated functionality to be offered as part of the company's corporate systems?

● *John Hookham is a director of management consulting and marketing services company Adrelia Ltd. Tel: +44 (0)20 7286 7073. Email: john.hookham@adrelia.com. Website: www.adrelia.com.*

● *If you would like more information about this article or any of the products or companies mentioned in the article, please contact us at [info@evaluationcentre.com](mailto:info@evaluationcentre.com).*