

Who Should Read This Brief?

If your company uses email to transmit any commercial information, regardless of size you may have a duty of care to ensure your emails and their attachments are retained in a tamper proof. This brief is suitable for business managers and IT staff.

For those contemplating deploying email archiving one of the most frequently asked questions is on the internal implications of being able to access and read potentially private, sensitive and confidential emails of employees. This whitepaper is for those organizations looking to deploy a Email Archiving solution and provides an insight into potential Human Resource implications for those looking to deploy such as solution.

Synopsis

Email is discrete and efficient form of communication and its growth as the primary form of communications is unquestionable. However as a consequence of its importance is the need to effectively and securely archive all incoming and outgoing emails.

However this is at odds with many peoples view of finding a balance in staff privacy when using company resources such as email. This paper highlights some of the issues and approaches; however it is not the substitute of appropriate legal advice.

Background

Traditionally companies had strong policies over the use of company resources for personal activities, most commonly personal telephone usage. However through the 1990s there has been a breaking of the tradition due to the demands of a more flexible working environment and the valuing of employees as companies move towards more service based industries.

Consequently individuals now expect and use email for personal and work activities. Contrary to this is the demand that management and legislation place on archiving, discovery and viewing of emails against private use of emails addresses.

Staffing Implications of Email Archiving

Regardless of a company's desire legislation often forces companies to deploy Email Archiving. For instance in the State of Victoria, Australia, all companies, regardless of size are required to be able to provide, "in a reasonable time" all emails that could pertain to any particular case on hand. The implication of this is that all emails should be archived, tamper proof and easily discovered.

Therefore it is important that clear policies are introduced, known and observed by all staff which applies to current and historical emails. As part of the process of deploying Email Archiving it is important to ensure that all staff whether new or existing understand and agree to having all emails archived and potentially revealed and read by a third party.

Recommendations to staff should be made that for personal and confidential emails a third party web based email service such as Google gmail or Yahoo should be used.

Should policies not be published and staff correctly informed there are serious risks, as outlined in one case involving a public-sector employee in 1999 who won \$5,910 in damages and \$11,820 in court costs and expenses after her communications were intercepted by her employer, Carmarthenshire College, based in South Wales. Lynette Copland successfully took the U.K. government to court after her personal Internet usage and telephone calls were monitored by one of her bosses.

The ruling means that the private use of company telecommunications equipment and Internet access may be protected under European human rights legislation, if the company has an acceptable personal-use policy and fails to inform employees *that their communications may be monitored*. Employee communications may also be covered by human rights legislation if the organization has no explicit acceptable-use policy and fails to inform employees of the monitoring of personal e-mail.

"According to the court's case-law, telephone calls from business premises are prima facie covered by the notions of 'private life' and 'correspondence' for the purposes of Article 8," said the court's ruling. "It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage. The applicant in the present case had been given no warning that her calls would be liable to monitoring; therefore she had a reasonable expectation as to the privacy of calls made from her work telephone. The same expectation should apply in relation to the applicant's e-mail and Internet usage."

In the United States, monitoring of employees' e-mail and other Internet communications is commonplace. *Some surveys have suggested that over half of large U.S. corporations currently monitor outbound e-mail or plan to do so.* Certain securities firms are subject to rules requiring them to save e-mail and instant messages and perhaps monitor a sampling of them.

Even in the U.S., though, the law isn't always that straightforward. If a company does not have a clear policy warning its employees that e-mail messages are subject to surveillance, courts may take a dim view of the legality of monitoring.

Provision of Email Usage Policies

Should you wish to develop an Email Usage Policy you can find an example at <http://www.mailrevive.com/resources> . Please note these as provided on an as-is basis. We recommend you consult with a professional advisor to clarify legislation in a particular country.

About MailRevive™

MailRevive™ is a managed application service that operates in conjunction with your existing IT network to ensure the protection, preservation and continuous operation of email communication for your business, while providing on-demand access for users anywhere and anytime. For any size business MailRevive™ will ensure that email data is automatically filtered and preserved, can be intelligently discovered, easily recovered and that continuous access is available at all times.