



Dan May of  
RAMSAC

### FURTHER INFORMATION:

|             |  |
|-------------|--|
| Commssoft   | <a href="http://www.commssoftuk.com">www.commssoftuk.com</a> |
| CTI Group   | <a href="http://www.ctidata.co.uk">www.ctidata.co.uk</a>     |
| OAK Telecom | <a href="http://www.oak.co.uk">www.oak.co.uk</a>             |
| RAMSAC      | <a href="http://www.ramsac.com">www.ramsac.com</a>           |
| Tri-Line    | <a href="http://www.tri-line.com">www.tri-line.com</a>       |

## User Checklist

Inappropriate electronic content in the workplace can lead to heavy fines and prison sentences for directors that fail to prevent pornography, and other unsuitable material, finding its way onto office desktops.

Dan May, Operations Director of IT consultants RAMSAC has provided Comms Business Magazine readers a checklist covering the policies, procedures and systems that need to be in place to prevent companies suffering at the hands of irresponsible employees.

**PUBLISH A CLEAR AND UNAMBIGUOUS ACCEPTABLE USAGE POLICY FOR INTERNET AND EMAIL.**  
*Give employees their own copy and display the policy in the office at a prominent location. Detail what material is considered unacceptable and what the repercussions could be for employees found in breach of the policy. Be firm but fair.*

**INCLUDE 'ACCEPTABLE ELECTRONIC SYSTEMS USAGE' IN ALL NEW EMPLOYEE LITERATURE.**  
*Make sure your Human Resources' function realizes the importance of communicating this message.*

**HAVE A STRUCTURED, ENFORCEABLE DISCIPLINARY PROCEDURE.**  
*Should you need to take action, make sure you can reference exactly which part of the acceptable usage policy the employee is in breach of.*

**IMPLEMENT SOFTWARE AND SYSTEMS THAT BLOCK ACCESS TO POTENTIALLY DANGEROUS WEBSITES AND EMAIL CONTENT.**  
*At the very least, any company with Internet access should have a firewall and anti-virus software installed. Content filtering software can be extremely cost-effective and can be configured to allow access to a limited range of websites.*

**WORK WITH YOUR IT FUNCTION TO DEVELOP A PC 'SCREENING' PROCESS**  
*Screen hard discs and server data stores for inappropriate content. This can pick up potential employee indiscretions before they become serious.*

**STANDARDIZE DESKTOP APPLICATIONS.**  
*By limiting employee access to only business-related software programs, you're removing channels through which they can access unsuitable content.*

**RESTRICT ACCESS TO THE INTERNET AT CERTAIN TIMES OF THE DAY.**  
*After-hours Internet abuse is a common problem. By removing access to PCs and the Internet out-of-hours, potential abuse of systems can be avoided.*

**IMPOSE RESTRICTIONS ON HOW MUCH CONTROL EMPLOYEES HAVE OVER THEIR PCS.**  
*If you're running a network, configure individual PC user rights so that only authorized employees can install and modify software. If not, make it company policy that employees do not modify their machines.*

**MAKE SURE ALL STAFF REALISE THE SERIOUSNESS OF THE ISSUE.**  
*How many people would walk down a busy street openly reading an adult magazine or bring such a magazine to work to read at their desks? Make sure your workforce understands the threat posed to their jobs – both by dismissal and business performance – of unsuitable electronic content appearing on PCs.*

## CRACK MONKEYS

Comms Business Magazine felt that a recent extract from Silicon.com's weekly roundup sums up the channel opportunity.

'As long as boffins find newer and cleverer ways to deliver new technology, so human beings will find newer and stupider ways to get caught out by it.

Consider the following cautionary tale. Two Prudential employees were this week fired for being a little less than prudent with the company's corporate email system. The two workers - believed to be a man and a woman - from the Pru's HQ in Stirling have been sacked after the financial services company decided email messages revealed they had been dealing

drugs at work.

According to reports in Scottish newspaper the Daily Record, police raided the couple's home and found quantities of amphetamines, cannabis and ecstasy. A further six employees are in hot water and have been subjected to disciplinary action after their names were found in the sacked employees' address books. (The names may or may not have been saved in a folder called 'crack monkeys'.)

It's staggering to think anyone would consider work email a secure communication medium for selling narcotics, especially given the media coverage about email monitoring and misuse of the internet in the office.'