

# Eat your Greens

## Implementing an Acceptable User Policy

Talking with a friend of mine the other day he jokingly told me of a situation in his company where when looking for details on a Canadian bank "Royal Bank of Canada, he miss typed the web address [wwwroyalbank.com](http://wwwroyalbank.com) missing the dot out after www. To his surprise, a porn site appeared on his computer screen.

There is of course a serious side to this event. What could have happened and how would it have affected his employees should they have had the same experience. This site would have clearly caused offence to some of his employees and undoubtedly, contravened any forward thinking or socially aware businesses Acceptable User Policy (AUP).

In business today, senior management and managers commissioned to take responsibility for the "acceptable use" of company computer resources have a heightened accountability to the business to ensure that protection from outside and indeed inside their organisation is fully maintained. With the latest legislation, it is now frankly unacceptable to use the excuse "I didn't know".

If we are to believe statistics from a number of experienced (Global) Security agencies that **70% of Misuse and Theft of Data comes from inside your company and leaves your company with serious threat of litigation**, then internet filtering and blocking is only managing to capture 30% of misuse and cyber slacking in today's modern environment. To put that in real terms, internet and e-mail facility abuse use at work costs the UK approx £10 billion each year.

So then why do we continue to watch the horizon and sit behind our outside barrier of firewalls? Instead, we should be proactively acting from the inside – using a combined approach of corporate and technology protection:

## **Corporate:**

Developing and enforcing an Acceptable User Policy (AUP), which provides all employees with a solid set of rules that clearly states what, when and how they are expected to use business communications.

## **Technology:**

Implementing the correct automated solution that monitors intelligently and without infringing employee rights, all incoming, outgoing and importantly, internally circulated communications including Instant Messaging (Hotmail) and Internet sites.

## **Policy Central Enterprise™**

Policy Central Enterprise is a unique "behaviour management" software solution for all businesses and organizations. It captures logs and reports all violations either in invisible operation mode or as part of an organisations agreed (AUP) practice. The intelligent violation engine enforces your (AUP) by monitoring all screen and keyboard activity, recording all violations via screen capture and maintaining a comprehensive audit log to provide detailed forensic evidence. It can be configured to monitor all Instant Messaging, Chat, Windows applications, documents and E-mail including all attachments. Once identified, the monitoring results can be utilised to implement Site Blocking or time management to Internet access and other applications again all within the Policy Central Professional environment.

## **KNOW WHAT YOU'RE DEALING WITH**

Knowing what risk is and what's at risk are the first steps in establishing a successful Acceptable User Policy (AUP). Understanding the myriad threats and vulnerabilities and keeping up with a shifting landscape are critical in maintaining a secure and safe operating organisation.

The rewards of a good AUP are difficult to discern at first. After all, it's difficult to point to things that didn't happen and call it a success. However, if the objective is to keep malicious events from happening, the lack of those events occurring is the barometer of an effective program's effectiveness.

To obtain an outline copy of AUP Guidelines and further details on Policy Central Enterprise, go to [www.forensicsoftware.co.uk](http://www.forensicsoftware.co.uk)



**Footnote:**

**[www.royalbank.com](http://www.royalbank.com) site has subsequently been closed down following a WIPO web judgement.**