

E-Surveillance - the facts and figures

A report based on a joint survey with *Personnel Today* magazine

Monitoring of employee use of e-mail and internet - the facts and figures

Executive Summary

The issue of e-mail and internet abuse at work has had a high profile over the past year, with some cases making national press headlines. When cases do hit the headlines, it is damaging to the company every bit as much as it is to the individuals. It is in everybody's interests to get the policy on e-mail and internet usage right, and to monitor and enforce it effectively.

Our survey, in conjunction with Personnel Today, found that while many companies appear to be making more efforts to monitor regularly and to let their employees know that they do so, the number of infringements of policy is still alarmingly high. Internet and e-mail abuse is a major disciplinary issue for any HR department and company.

Key findings

1. Policy

Encouragingly, the great majority of companies have clear guidelines for employee behaviour which define 'misconduct' or 'gross misconduct':

- 93% of companies do have guidelines for employee behaviour
- 93% of these communicate this policy to all employees
- 87% of these policies include definitions for 'misconduct' or 'gross misconduct'

From the 172 companies whose policy does include definitions of 'misconduct' and 'gross misconduct', the following separate issues were expressly addressed:

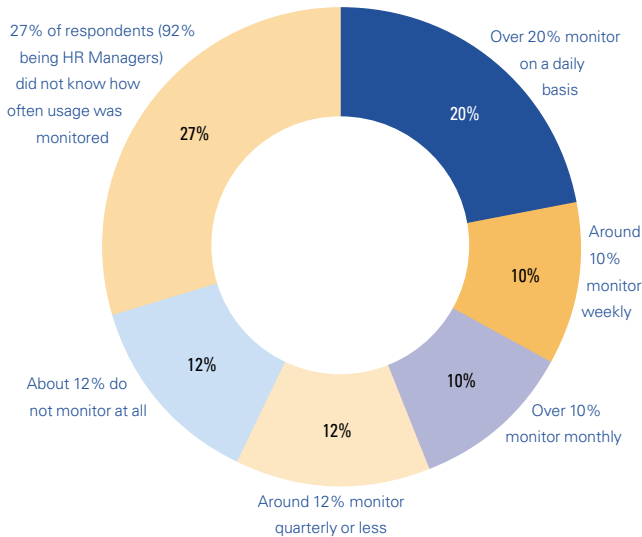
- 132 times - Acting dishonestly
- 130 times - Violence or criminal activity
- 117 times - Sending any e-mail that is pornographic in nature
- 115 times - Breach of health & safety rules

Company policy on email and internet access and on permissible levels of personal use vary quite considerably:

- 54% allow all staff access to the intranet, 49% to the internet and 63% to email.
- 10% of companies have a total ban on personal use of e-mail and 13% on personal use of internet. 14% have no usage policy for email and 13% have no usage policy for internet.
- 29% of employers do not allow employees to use email for personal use during contracted working hours. 35% of employers do not allow employees to use the internet during contracted working hours.

2. Monitoring

Monitoring employee use of e-mail and the internet is vital if the company's policy is to be effectively implemented. Frequency of monitoring varies considerably however:



In terms of communicating the monitoring policy, 73% of companies said that they do make employees aware that they monitor email and internet usage. 6% admitted they do not, while 7% of respondents did not know whether they did or not. 12% do not monitor at all.

The responsibility for ensuring that employee monitoring does not breach Data Protection laws rests with HR Departments in 42% of cases, with the Board taking responsibility in 16% of cases.

3. Implementation

Overall in the last 12 months there have been 358 disciplinary cases and 61 dismissals for e-mail and internet related offences. The most common amongst these were:

- 69 individuals have been disciplined for excessive amount of time using the internet or email for personal use and 5 were subsequently dismissed.
- 64 individuals have been disciplined for sending e-mails that are pornographic in nature. 25 individuals were subsequently dismissed.
- 53 individuals have been disciplined for accessing websites which may contain pornographic material. 9 individuals were subsequently dismissed.
- 49 individuals have been disciplined for sending emails that may damage the company's reputation. 2 individuals were subsequently dismissed.

4. Prevention

Many companies are not making use of software and firewalls to prevent inappropriate e-mail and internet use.

- Only 53% of companies have software to prevent access to inappropriate websites
- Only 71% have firewalls to block inappropriate e mails
- 11% of companies with software and firewalls in place are not confident that it works

Implications for Business

1. The Law

Companies need to be aware of the series of statutes that have been introduced governing surveillance. These are:

The Data Protection Acts 1984 and 1998 – The Act regulates the acquisition, processing and storage of data and gives the individual certain rights, including the right to inspect and challenge both misuse and inaccuracies.

The Human Rights Act 1998 – Until the Act came into force in October 2000, people in the UK had no express right to privacy. The Act has now introduced the possibility that protection for private and family life will limit the company's right to monitor. The law in this area will develop rapidly.

Regulation of Investigatory Powers Act 2000 – The starting point here is that, unless specifically permitted by the Act, an interception is unlawful. Where the legality of an interception is doubtful, an employer must demonstrate reasonable grounds for believing that both sender and recipient have consented to monitoring.

2. The Responsibility

Companies need to have clearly defined roles and responsibilities to ensure that monitoring, enforcement and communication of e-mail and internet policy are both effective and compliant with the law.

Only 16% of Boards take responsibility in ensuring that Data Protection rules are not broken. With the potential consequences for breach of individual rights so high, Boards should perhaps ask themselves whether they need to be getting more closely involved.

Conclusion

It is perhaps a shock to discover that the number of disciplinary cases in the last 12 months for e-mail and internet abuse is greater than the number of cases for dishonesty, violence and health and safety breaches combined.

The problem of e-mail and internet abuse at work is certainly not going away. If companies are monitoring more closely and frequently, it does not appear to be deterring people from abusing company systems.

Communicating monitoring policies more directly and forthrightly, as well as investing in better software and firewalls, could help companies to combat this problem more effectively.

For further information please contact:

Stephen Levinson, Partner

KLegal, London

Telephone +44 (0) 207 694 2652

Email stephen.levinson@klegal.co.uk