

White Paper

Employee Internet Access

Effective Management of the Organisational Risk

Published by: *NET*consent Limited

Publication date: March 2004



Table of Contents

1.0 Foreword	4
2.0 Introduction.....	5
3.0 Current Legal Situation	7
3.1 Liability	7
3.2 Regulation of Investigatory Powers Act 2000.....	8
3.3 Data Protection Act 1998	9
3.4 Office of the Information Commissioner	10
3.5 Human Rights Act 1998	10
3.6 Freedom of Information Act 2000.....	11
4.0 Employee Internet Policy Management.....	12
4.1 Trust	12
4.2 Contract of Employment	12
4.3 Paper Policy with Employee Signature	13
4.4 Communication via Company Intranet and Pop Up	13
4.5 Authorised Access	14
4.6 EIPM Software.....	14
5.0 Employee Internet Management.....	15
5.1 Solutions.....	15
5.2 Benefits	16
6.0 Conclusion.....	17
7.0 Further Information	18

1.0 Foreword

This white paper was written by *NET*consent Limited, together with Websense Inc. *NET*consent is a leading vendor of effective policy management software solutions and Websense is the worldwide leader of employee internet management solutions.

The document aims to outline the current legal situation that organisations find themselves in, when allowing their employees to access the Internet in the workplace. It also gives guidance on how organisations can best protect themselves against the risks that this creates, in a practical and cost effective manner.

The information contained in this white paper was correct at the time of publication. *NET*consent endeavours to ensure that the information in this white paper is correct and fairly stated at the time of publication, but does not accept liability for any error or omission.

The document should be read not only by IT professionals with responsibility for the network and systems which allow Internet access in the workplace, but also by professionals from other functions, including directors with legal responsibility for corporate governance and compliance, as well as HR professionals with responsibility for the rights of the employee in the workplace.

2.0 Introduction

The creation and development of the Internet has been the most astonishing aspect of late twentieth century society. Its effects have been far-reaching and profound, not least in the work place.

Employees can now complete tasks, which used to take hours, in seconds. They can use email to communicate almost instantaneously with customers and colleagues at remote offices and can use the World Wide Web for purposes such as research into markets, customers and competitors.

More and more organisations are utilising Web technology to share information with their employees and partners in the supply chain. The explosive growth in corporate intranets and extranets is testament to this and it is now estimated that 260 million employees worldwide have access to the Internet at their workplace.

Improvements in productivity for the business are obvious. However, as access to the Internet becomes more widespread, the temptation for employees to misuse this resource has also grown. The connection in the workplace may be many times faster than at home and the lure of free music and videos proves too great for many to resist. There has also been a growth in employees using corporate resources to host personal applications, for example the very popular peer-to-peer file sharing programs such as Kazaa and Morpheus. The problems appear to be getting more prevalent and more serious, with the biggest single disciplinary issue at work today being abuse of the Internet.

Organisations taking advantage of this new technology to help them to manage their business also have to consider that they may be inadvertently allowing access to their business critical information, potentially of great value to a competitor, to anyone connected to the Internet.

Access to the Internet was initially an issue dealt with solely by IT professionals, implementing systems to allow users to access information and installing firewalls to prevent external hackers gaining unauthorised access to the corporate network. However, responsibility has now widened and includes professionals from other functions, including directors with legal responsibility for corporate governance and HR professionals with responsibility for the rights of the employee in the workplace.

The legal landscape in the UK has also changed significantly over the last 10 years, as legislators have sought to catch up with the advances made in technology. New legislation is being implemented regularly, mainly concerning the rights of the employee and the responsibilities of the employer. Legislation, which must be considered, includes the Human Rights Act 1998, the Data Protection Act 1998, the Regulation of Investigatory Powers (RIP) Act 2000 and advisories on monitoring employee Internet access being issued by the Information Commissioner.

The methods of regulation of employee Internet access by many organisations are often ad hoc and outdated. Those that have actively chosen to address the issue have done so by creating a corporate Acceptable Usage Policy (AUP), for Internet use.

This AUP can be distributed in a variety of ways, ranging from the distribution and signature of the policy on paper to the implementation of Employee Internet Policy Management software. In most organisations this process is not managed well, with many exceptions occurring, for example, when a new employee joins just after a policy has been rolled out or a temporary employee joins for a short period of time. A common problem is that policies are allowed to become out of date and do not change, for example when new legislation is introduced. This is often because distributing and getting agreement to new policies in the traditional manner is too time consuming to be practical.

This relaxed attitude to the distribution of and agreement to corporate Acceptable Usage Policies is a high risk strategy, as was highlighted by the recent case brought by Bob Clarke, a former employee of TXU Energy. Clarke had been sacked after sending an email which was deemed to be racist and sexist by TXU Energy. He claimed that the email was intended as a joke and was not meant to cause offence. He also claimed that the company had never informed him what types of email were allowed, a fact confirmed by a number of his former colleagues. An Employment Tribunal decided that although the email was inappropriate, Clarke's dismissal was unfair, because he had not been informed of any corporate Internet Acceptable Usage Policy and had not been given a warning. He was awarded £32,000 in compensation.

In order to prevent this situation arising, organisations should ensure that their employees are not able to access the Internet without first reading and agreeing to the corporate AUP. Should a new policy be introduced, access should automatically be blocked until the user has read and agreed to the new or updated policy.

Not only is the principle of agreement by employees to an AUP important, but also once they have agreed, management, monitoring and reporting on their Internet access is critical. To ensure that employee productivity and corporate stature are maximised and legal liability minimised, integrated solutions managing policy deployment, blocking access to inappropriate web sites, managing bandwidth, allowing effective auditing and reporting, all aligned around a strong and universally distributed AUP, are essential.

3.0 Current Legal Situation

3.1 Liability

The question most organisations have to face, when considering the current legal landscape surrounding employee Internet access is, where will any liability arise? This issue can be broken down into two key risk areas, employee breach and employer breach.

Examples of where Employees are most likely to breach the law are:

- Inappropriate use of the Internet / email: An employee downloading illegal files, such as offensive images or pirated software
- Harassment: An employee viewing a web site containing inappropriate images in front of colleagues, which causes them offence and could be considered to be harassment
- Defamation: An employee posting a libellous comment about a third party, on an Internet message board
- Confidentiality & trade secrets: An employee posting confidential information about an organisation on an Internet message board or sending it by email to a competitor, that they may be about to join
- Damage to reputation: Articles appearing in the press about employees being fired by an organisation for viewing inappropriate web sites during working hours. Several organisations have found themselves in this position over recent years

Examples of where the Organisation is most likely to breach the law are:

- Inappropriate / unjustified monitoring: When employees are being monitored and their communications are being intercepted without their knowledge or consent
- Data protection compliance: Where information is being gathered about an employee and their use of the Internet, but is not kept secure or is held for a longer period than is necessary
- Employment law: Where an employee is fired for breaking the company Internet Acceptable Usage Policy, but the employee has never been made aware of the AUP at any time. Former employees have been able to use this argument when successfully suing for unfair dismissal
- Liability for employees: Vicarious liability arises where the wrongful action is not primarily attributable to an organisation itself, but the law nevertheless holds the employer responsible for the misconduct of its employees. Also, the actions of an employee, such as entering into a contract or making a statement, can bind the organisation externally

The main pieces of legislation, which apply in the field of Employee Internet Management, are the RIP Act 2000, the Data Protection Act 1998 and the Human Rights Act 1998. The Office of the Information Commissioner has also issued guidelines as to how organisations should proceed in order to ensure that they comply with the current legislation. A brief summary of these Acts and the issues that they raise is given below.

3.2 Regulation of Investigatory Powers Act 2000

The RIP Act 2000 came into force in October 2000 and regulates the interception of communications made via public postal systems, public telecommunications systems and private telecommunications systems. The RIP Act makes it an offence to "intentionally and without lawful authority" intercept communications in the course of their transmission. The RIP Act 2000 repeals the prior legislation in this area, the Interception of Communications Act 1985 and widens considerably the organisations covered by legislation. The Act intersects with the Data Protection Act (1998) and the Human Rights Act (1998) against which any action under the RIP Act must be balanced.

This legislation attempts to provide a clear framework for the lawful interception of communications by both public and private organisations and was introduced as a response to recent technological advances and concerns about new methods of monitoring communications that these advances allow. It is now unlawful for individuals and organisations other than certain state bodies to "intentionally and without lawful authority...intercept, at any place in the United Kingdom, any communication in the course of its transmission" (this applies to both public and private systems).

A person intercepts a communication in the course of its transmission if he so modifies or interferes with the system, or its operation, or so monitors transmissions made by the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication

However, the RIP Act does allow for certain legitimate interceptions of communications by organisations on their networks and provides "lawful authority" for these.

What is lawful authority? Monitoring can take place with the consent of both the sender and the recipient but this may be difficult to achieve in practice, for example from external senders of email. Other rules for legitimate interceptions are mainly to be found in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The interception has to be by or with the **consent** of a person carrying on a business, for purposes relevant to that person's business, and using that businesses own telecommunications system.

The interception of business communications for business purposes, must be for one of the following reasons:

- To establish the existence of facts
- To ascertain compliance with applicable regulatory or self-regulatory practices or procedures
- To ascertain or demonstrate effective system operation, technically and by users
- For national security/crime prevention or detection
- For confidential counselling/support services
- For investigating or detecting unauthorised use of the system
- For monitoring communications for the purpose of determining whether they are communications relevant to the business

The system controller must also have made all reasonable efforts to **inform** every person who may use the system that there may be interception. As yet, however, the courts have not had the chance to decide what exactly constitutes “reasonable” in this context.

A general exception is made in the RIP Act for interception where it is by a person running a telecommunications service and for purposes connected with the provision of that service. For example, email may be examined when misaddressed in order to redirect it as necessary, or email subject lines may be checked, to filter out viruses. While this may mean that the postmaster sees some of the content of the message, the Act makes it clear that there is no requirement on the network operator to give warning of the possible loss of privacy in such circumstances. System operators may also monitor network traffic in order to determine its source, where this is necessary to ensure the effective performance of their mail servers, for example to eliminate ‘spam’.

3.3 Data Protection Act 1998

The Data Protection Act 1998 came into force in March 2000 and regulates the processing and handling of personal information that has been obtained lawfully.

The Act applies to data collected from which it is possible to identify a living individual, either on its own or in connection with other data. This includes the disclosure of communications data, whether under the RIP Act or any other statutory or common law regime, such as data obtained whilst performing any of the following:

- Monitoring of employee communications
- Monitoring of employee Internet use
- Any investigation of Internet abuse

Organisations processing personal data must comply with the data protection principles set down in the Data Protection Act. These require data to be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with individuals' rights
- Kept secure
- Not transferred to non-European Economic Area countries without adequate protection

A number of conditions are set down within the Act, relevant for the purposes of the first principle, and every employer, as a data controller, must meet one of these conditions in order to legitimise its processing. One of these conditions is that the data subject has given his consent to the processing. Where the employer processes sensitive personal data such as on health or racial origin, an additional justification must be found. Failure

to comply with the Data Protection Act can lead to enforcement action by the Information Commissioner as well as to an individual taking the data controller to court to claim compensation.

3.4 Office of the Information Commissioner

The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000. The office was set up in order to help employers comply with legislation and to adopt good practice. It does not impose any new legal obligations. The Commissioner reports directly to the UK Parliament and has an international role as well as a national one. The Information Commissioner has issued a Code of Practice on Employment and the latest part; Part 3 is concerned with monitoring employees at work.

The advice given in the Code of Practice recommends that employers:

- Establish a policy and communicate it to workers
- Comply with current legislation and make an impact assessment to decide if monitoring is justified
- The Commissioner recommends taking a minimalist approach, for example, reviewing traffic data and subject headings before content and recommends where possible to make monitoring automated, to ensure privacy is not infringed
- The Commissioner recommends consultation, notification and reminding of employees to ensure that they are aware of any monitoring
- The Commissioner also recommends that covert monitoring should not normally be considered as it can rarely be justified and should only be used in exceptional circumstances. Where it is used, it should be ensured that it is strictly targeted at obtaining evidence within a set timeframe and that after the investigation is complete the monitoring should cease

3.5 Human Rights Act 1998

The Human Rights Act 1998 came into force in October 2000 and incorporates into UK law certain rights and freedoms set out in the European Convention on Human Rights. The Act includes 18 articles, the most relevant of which within Employee Internet Management is Article 8, which is the Right to Respect for Private and Family Life. This is broken down into two parts in the Act.

- Everyone has the right to respect for his private and family life, his home and his correspondence
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others

Article 8 clearly has to be considered when monitoring employee communications and an employer should not routinely be reading private correspondence relating to their employees' private and family life.

3.6 Freedom of Information Act 2000

The Freedom of Information Act 2000 received Royal Assent on 30th November 2000 and will be fully implemented by January 2005. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector. It provides clear statutory rights for those requesting information together with a strong enforcement regime.

The legislation will apply to a wide range of public authorities, including Parliament, Government Departments, local authorities, health trusts, doctors' surgeries, publicly funded museums and thousands of other organisations. The main features of the Act are:

- A general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions
- In most cases where information is exempted from disclosure there is a duty on public authorities to disclose where, in the view of the public authority, the public interest in disclosure outweighs the public interest in maintaining the exemption in question
- A new Information Tribunal, with wide powers to enforce the rights will be created
- A duty is imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the Commissioner, will specify the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee

This should be borne in mind by the public sector as it could mean that their policies and procedures become publicly available.

4.0 Employee Internet Policy Management

It is important that once a corporate AUP has been created, it is communicated effectively and comprehensively to all employees. If just one employee accessing the Internet in the workplace is unaware that the organisation has an AUP or has not been given the opportunity to read it, significant risk for the organisation is created.

When communicating the AUP to employees, it is important that the method used follows certain important guidelines.

- Employees should not be allowed to access the Internet unless they have agreed to the current AUP
- New policies, taking into account new legislation which has come into force for example, must be rolled out quickly. It is important that new policies are not delayed by the bureaucracy of distribution and agreement
- It is important that employees take the time to read and understand the policy and are not just signing or clicking the "OK" button without bothering to read the text of the policy
- It is important that employee agreement to corporate AUP's is fully auditable. It should be easy to access information such as, who has agreed to which policy and on which date
- It is important that the identity of an employee can be validated when agreeing to the corporate AUP, in order to stop an employee agreeing to a policy by clicking OK, for example, when at the work station of a colleague

There are several ways in which organisations currently choose to communicate their Internet Acceptable Usage Policy to their employees. Examples of these are:

4.1 Trust

Many organisations rely on trust, when allowing their employees to access the Internet in the workplace. The benefits of this are that the company is able to portray a relaxed working atmosphere and can avoid any cost or time spent in developing and rolling out a policy. The drawbacks of this method of EIPM are almost too many to list, ranging from employees being unaware of what is considered to be appropriate behaviour, through to employers being unable to legally monitor their employee's Internet access in the workplace. Former employees have even been able to successfully sue for unfair dismissal after being fired for inappropriate use of corporate Internet resources, their defence being that they were unaware that their activity was in contravention of corporate policy.

4.2 Contract of Employment

Some employers do make a limited effort to manage the relationship with their employees through their contract of employment. During induction, the employee is introduced to company procedures and practices and is perhaps required to sign various

documents, which may refer to corporate policy at that time. In certain instances, the employment contract may require the employee to comply with, at the time, amendments which may be introduced at some future date. Once again this approach is flawed. For example, a court case may rely on employee knowledge of a specific clause in the corporate AUP, which the employee is genuinely unaware of, since it was introduced after their induction and they have not been informed of the change.

4.3 Paper Policy with Employee Signature

Creating an AUP and distributing it on paper, for employees to sign and return is an important advance on the first two methods of managing employee Internet access as described above. Some employee involvement in the process of creating the policy is advisable, as this will enhance the value of the policy and ensure that it is 'fair', 'open' and 'democratic'.

There are several drawbacks in this method however. It does require a high investment of time to physically print out, distribute, collate returns, chase non-returns and archive signed policies. One organisation estimated that this process took 17 man days within their 500 user organisation.

The fact that users can access the Internet before they agree to the policy has to be considered and they may be doing so in a manner which contravenes the new policy, but of course there can be no sanction.

The effort required to maintain accurate and updated records reflecting the changing pattern of staff – leavers, starters and the use of temps and contractors also has to be considered, not to mention the fact that the effort is likely to need to be repeated on several occasions as new legislation comes into effect or new technology comes to the fore and corporate policies are changed to take account of this. What actually tends to happen is that management are reluctant to invest in the process again and a period of time passes when users are not covered by an up to date AUP.

4.4 Communication via Company Intranet and Pop Up

To overcome the time and cost implications of distributing policies by the 'traditional' paper based methods, the organisation may try to utilise electronic methods of distribution. Some typical examples are:

- Communicating the AUP by placing it on the corporate intranet, potentially available to all staff with access to a PC
- Communicating the AUP utilising a pop up containing the policy statement, every time users log on to the network or begin a particular transaction sequence such as accessing the Internet

These methods of communication are essentially one way, without valid evidence of employee, or user, acceptance or agreement to comply with the statement or even of having read the policy statement. Even if the user is required to click to indicate 'acceptance', there will be little added value unless the click transaction is recorded, or if

anyone sitting at the workstation can click OK without evidence of who that user actually is. If the pop up appears, or the intranet routine is inserted, for every occasion, it will be seen by the user solely as an added layer of bureaucracy.

4.5 Authorised Access

An alternative solution adopted by some employers requires the employee to initiate a request to access the Internet. Access will be allowed supported by a signed agreement to comply with the AUP, with senior management approval. On receipt of the approval, the IT department is authorised to allow the employee to have Internet access. This creates a heavy burden on the IT department, having to take time out to allow each new user Internet access. There are also other serious questions for management to address. For example, when a new policy is introduced, as it must be to take into account changes in the law and technology, should all prior management authorisations be revoked and all internet access be suspended by IT action, perhaps only to be reversed en masse on the new policy's first day of application? And what would the cost of this be to the business in terms of lost productivity?

4.6 EIPM Software

The most effective solution to the problem of enforcing the organisation's Internet Acceptable Usage Policy is EIPM software. This type of software is currently the only solution which addresses effectively the five points listed at the beginning of section 3. Once a new policy is available for deployment, due review of the policy having been completed and authorised, it will be electronically distributed to all staff when they first attempt to access the Internet. Once it is presented to staff for review and acceptance, then no access is permitted until acceptance is keyed in and the user's identity is verified using their network user name and password. Once the user is verified then access is granted to the Internet.

In order to reduce the IT overhead, authority can be given to managers in other departments such as HR, to revoke individual access, when circumstances require. If for example, it is identified that a user is attempting to access the Internet to surf inappropriate web sites. Also reconnection can be allowed through management action, rather than IT, if after review, such action is deemed appropriate.

EIPM software allows organisations to adopt a strategy of dynamic policy management. A company can easily refresh policies as and when required to ensure that they are always in line with current company procedures, new technology and legislation requirements.

It is essential that once a policy has been introduced and agreed by users, that a history of transactions by employees is created and updated as policy updates are released. This history should include a record of all policies with dates of deployment and when superceded. Reports should be easily accessible in line with the requirements of management and auditors, internally or for BS7799 accreditation, for example. These reports provide relevant evidence where disciplinary action is to be initiated which may escalate to resolution by tribunal.

5.0 Employee Internet Management

5.1 Solutions

Once users have agreed to an AUP and employees are allowed to access the Internet, certain threats and risks become evident, for example, the risk of employees surfing the Internet for large parts of the day rather than working, or of employees surfing inappropriate web sites. There is also the risk of employees downloading programs from the Internet, which may be illegal, such as music and video files. There is also the risk of employees downloading viruses onto the network which could cause major disruption to the operation of the organisation and damage to their reputation.

The most effective way to control employee access to inappropriate web sites is by the use of URL filtering software. This software checks any Web page that the employee attempts to access against a list of categories, such as sports, adult material etc. The software then blocks access to the page if the employee does not have authority to view sites in a category. There are a variety of products available on the market which aim to achieve this and any selection process for such products should be comprehensive and rigorous, given the risks to the organisation.

All requests for Web pages should pass through an Internet control point such as a firewall, proxy server, router, network switch or caching appliance integrated with the URL filtering software. The product should also work from a very large, flexible and effective database of web sites, broken down into effective categories so that blocking of web pages can be done according to the existing culture within the organisation. The more effective the database is, the lower the risk that sites containing viruses, offensive material and pirated software will be visited

With customisable Internet filtering options, management of Internet use can adapt to the corporate environment. Whether it is decided to define use by user, group, workstation or network, and block, limit or defer access, the product selected should be able to accommodate specific needs.

The selected product should also have highly effective reporting built in. A comprehensive and easy-to-use reporting tool will help to evaluate employee Internet use and risk. Trend, summary or detail reports will then help identify any possible Internet access issues related to network bandwidth, legal liability, productivity and network security.

The chosen product should offer a wide range of policy options, which will allow IT administrators to carry through corporate policies. They should allow for time-based quotas, to allow users a set amount of personal web surfing each day. Not only is this flexibility popular with users, it also reduces the amount of time required to be spent by IT administrators, since less requests for help are made. This obviously reduces the support overhead and long-term costs.

Organisations have to consider the efficacy of their URL filtering program seriously. Purchasing an inferior product could result in an organisation breaking the law if, for

example, an employee is viewing a web site that should have been blocked and a second employee sees the offensive content on the screen, the organisation can be found liable for not adequately protecting the second employee from exposure to such material. A single lawsuit can easily eat up the money that would be saved by buying an inferior product. The cost of firing an employee who has been looking at offensive websites, which were not blocked by the inferior URL filtering tool, would also be expensive, not to mention the cost of hiring a replacement.

The product must be mature and fully tested and integrate seamlessly with other security systems, such as firewalls, which are already in place within the organisation. Companies that cannot compete on features or customer references often use low prices as a means to win business, but a system which fails periodically, not only opens up all the risks inherent from unchecked web access, but it will also consume resources within the IT department as any problem that occurs will have to be fixed. Organisations should require a solution that is widely used by the top companies. One that has had a number of versions, improvements, upgrades for example.

Another important factor is that the company, which is supplying the URL filtering software, should be financially strong. For example, if purchasing a product with a multi year agreement, it is imperative that the filtering company remain in business throughout the duration of the agreement. If they do not, not only is there a financial loss from the purchase of the product, but there is also lost time in the set up period and in the time taken during the selection process that has to be run again.

5.2 Benefits

The benefits in productivity of efficient employee Internet management are clear, but there are also bandwidth and legal issues to consider. For example, one of the most commonly pirated and distributed pieces of software is Adobe Photoshop, which is more than 100Mb in size. Even with a fast Internet connection these files can take a long time to download and drain bandwidth. A further unseen cost is that IT departments are often called upon to support these applications, taking them away from genuine projects.

Of course, wasted bandwidth is nothing compared to the destruction that can be unleashed by a new computer virus. Because hackers often tamper with pirated programs, many of these software packages contain hidden executables or viruses.

Perhaps the most obvious reason why corporations should be concerned about pirated software in their workplaces is the fact that it is illegal. Another rarely reported legal implication of pirated software is its strong link with online pornography. When viewed by an offended co-worker, these inappropriate photos have in the past resulted in sexual harassment or hostile workplace lawsuits against the organisation involved.

The four key benefits of using best of breed URL filtering software are:

- Increased productivity
- Decreased legal liability
- Conservation of corporate resources, such as bandwidth and IT time
- Decreased risk of viruses which can cause severe disruption

6.0 Conclusion

In today's competitive market place, employers have many calls on their resources, financial and otherwise and directors, personally, have a legal requirement to address a range of governance and diligence responsibilities.

In this white paper, the responsibilities of the Employer, whose staff have access to the Internet at their place of work, have been presented in terms of the current raft of related legislation – Data Protection, Regulation of Investigatory Powers, Human Rights, Freedom of Information and the recommendations published by the Information Commission.

Corporate policy communication with all staff should be on a two-way basis, and should be an on-going process with regular review to ensure continuing relevance in an ever changing business environment, absorbing changes in legislation, advancing technology, evolving internal working practices and social expectations.

Compliance with the organisation's policies should be subject to an audit programme with due review of the reported findings.

Allowing Internet access in the workplace is double edged sword – it enables significant productivity gains, but carries a significant financial risk if misused by the organisation's employees. If the organisation is to achieve the benefits of an enlightened management in the exploitation of the Internet, the following is advised -

- The organisation's Acceptable Usage Policy should be universally deployed, with access to the Internet only granted when staff have been made aware of and agreed to the policy
- Internet Access should be managed via a highly effective URL filtering tool, with the capability both to regulate in accordance with the corporate AUP and to generate an appropriate level of reporting in order to facilitate effective enforcement

7.0 Further Information

For further information on managing the organisational risks presented when allowing employees to access the Internet in the workplace please contact your chosen *NET*consent partner. A list of these can be found at: <http://www.netconsent.com> on the how to buy page.

Alternatively contact:

*NET*consent Limited
82 Park Street
Camberley
Surrey
GU15 3NY
United Kingdom

t: +44(0) 870 013 1600

f: +44(0) 870 013 1601

e: info@netconsent.com

w: www.netconsent.com

For further information from vendors of the market leading tools for managing corporate Internet Acceptable Usage Policies and Employee Internet Access visit:

w: www.netconsent.com

w: www.websense.com

Notes



82 Park Street, Camberley, Surrey, GU15 3NY, United Kingdom
t: +44 (0)870 013 1600 f: +44 (0)870 013 1601
e: info@netconsent.com w: www.netconsent.com