



The **Threat** of **Lifestyle Computing** in the **Enterprise**

Creating clear delineation between personal devices & corporate IT assets

device**wall**TM
from Centennial Software

A guide from Centennial Software
October 2005
Issue 1.2

Contents

1.	New technology, new opportunity, new threat?	3
2.	Closing the security gap	4
	2.1	Why do you need an acceptable use policy?	
	2.2	Vicarious liability	
	2.3	The trouble with policies	
	2.4	Not all policy breaches are deliberate	
	2.5	But some are...	
3.	Re-focusing on areas of unaddressed risk	7
4.	What are the risks?	8
	4.1	iPods and music players	
	4.2	USB sticks and memory cards	
	4.3	PDAs and mobile phones	
	4.4	Categorising risks	
5.	Establishing permissible use	10
6.	Revising your security policy	11
7.	Deploying and communicating the policy	12
8.	Enforcing the policy	13
	8.1	Introducing DeviceWall	
	8.2	Using DeviceWall to support permissible use	
	8.3	Temporary access requirements	
	8.4	Deployment	
	8.5	DeviceWall at work	
9.	Conclusion / Summary	15
10.	Appendix	16
	A1	Checklists	
	A2	Sample Acceptable Use Policy	

1. New Technology, New Opportunity, New Threat?

Over recent years, the proliferation of personally owned 'lifestyle IT'* devices such as PDAs, music players, digital cameras and mobile phones has been phenomenal. Falling costs, increasing choice, and overlapping functionality mean that these items are now well within the reach of most of the adult population. This in turn has led to their increasing presence in the workplace, often employed for both personal and professional uses.

While often these devices are purchased to host personal data, they can just as easily be used to carry sensitive business information such as contact details, appointments, email, work in progress etc.

At first glance, this blurring between personal IT and corporate data may not seem like an issue, but the lack of control over devices and data poses a significant risk to businesses that are ultimately accountable for their intellectual property in terms of manageability, security and confidentiality.

This risk is amplified by the sheer diversity and speed of connections that can now be used to transfer content to and from these devices from corporate PCs – from the ultra-fast USB2 and Firewire connections to wireless technologies such as infrared and Bluetooth.

What's more, while many of these devices are marketed as being ideal to hold a particular type of content (music files, appointments, contacts etc.) the truth is that the majority can hold data in a vast variety of formats (an iPod will just as happily hold Word documents as MP3 files).

As such, a device that is intended to be used to synchronise diaries for field staff or even innocently play music is also capable of copying and storing corporate databases such as prospects, client personal data or the like in a matter of seconds (taking valuable information from a business), or introducing a threat onto the corporate network (in the form of a virus, spyware, inappropriate content etc).

"A company's biggest security threat isn't the sinister hacker trying to break into the corporate network, but employees and partners with easy access to company information... For more than a decade, corporations have erected digital perimeters to keep outsiders off their networks. But now discontented, reckless and greedy employees, and disgruntled former workers, can all be bigger threats than the mysterious hacker. And as more companies outsource portions of their business, vital company information can easily fall into the wrong hands."
'Securing data from the threat within',
ZDNet, January 11 2005

"The iPod may be popular, but also poses such a major security risk for businesses, that enterprises should seriously consider banning the iPod and other portable storage devices, according to a study by research firm Gartner Inc."

iPods pose security risk for enterprises, InfoWorld, July 06 2004

** 'Lifestyle IT' is defined by Centennial Software as the use of technology (often designed for 'home' use) to manage and improve personal efficiency.*

2. Closing the security gap

A survey of over 100 organisations in key economic markets showed that concerns over data protection, security and IT governance are now the clear leaders in terms of perceived business risk.

It's easy to understand why. One need look no further than both the popular and specialist press for high profile examples of where misuse of IT has led to difficulties for organisations.

The risks that businesses face as a result of the misuse of their IT infrastructure are generally well documented. They include:

- 🔗 Loss / theft of confidential information
- 🔗 Breach of intellectual property rights
- 🔗 Disruption through virus or malicious code
- 🔗 Misuse of corporate network and IT assets

For the majority of organisations, defence against these threats comprises a combination of external and internal security measures. To guard against external threats, firms have invested huge sums in security technologies such as firewalls, anti-virus, content filtering solutions and intrusion detection.

In contrast, internal security measures at the desktop rely largely on Acceptable Use Policies, designed to shape employee behaviour in such a way as to minimise the likelihood of security breaches on the network.

The proliferation of 'lifestyle IT' devices, together with the ease with which content can be transferred to and from PCs within the 'safety' of the corporate network, presents arguably the greatest prevailing risk to the corporate network today. Companies need to have a clear understanding of this emerging threat and have a robust policy on the subject and ability to enforce it.

2.1 Why do you need an Acceptable Use Policy?

As a matter of sound corporate governance, an organisation needs to protect its interests (as well as those of its shareholders, customers and employees) against the inappropriate use of corporate assets, especially in the areas of Information Technology. As such, businesses need to set, communicate and enforce policies on acceptable use of these assets and the information they access.

An Acceptable Use Policy is a common method for setting clear boundaries between the employer and employee on what is permissible and what is not in the corporate IT environment. The policy should leave employees in no doubt as to what is expected of them when they are on the network, and should spell out the disciplinary consequences that will result if a staff member does not comply with it.

"94% of large business suffered a security incident in 2004. The average cost of a single security incident to these companies was £120,000."

Information Security Breaches
Survey 2004

This policy, providing it is well drafted and effectively communicated to all employees, should afford the organisation some level of comfort that its systems will not be deliberately misused and that the firm is taking reasonable steps to absolve itself for any liability arising from inappropriate activity on its network.

2.2 Vicarious Liability

The need to manage the risk associated with inappropriate actions – especially the misuse of systems by employees – is made all the more pressing due to the legal concept of ‘vicarious liability’.

Put simply, vicarious liability states that an organisation and its Directors carry a personal responsibility for the actions undertaken by its employees in the course of their work – regardless of whether that action was sanctioned by the firm or not.

An Acceptable Use Policy is one mechanism that organisations can employ to help reduce the risk of vicarious liability, but this is by no means a panacea and there are some serious shortcomings that must be addressed through other means.

2.3 The trouble with policies

While Acceptable Use Policies can be an effective tool to help organisations reduce the number of malicious or accidental security breaches, the reality is that they are often far less than effective. Policies frequently suffer from:

- ☞ Poor drafting or inadequate scope
- ☞ Lack of communication with employees
- ☞ No affirmation that employees have understood and signed-up to the policy
- ☞ No periodic review of policy to reflect changing habits and technologies
- ☞ Lack of enforcement

All of which can render the effort that went into preparing and distributing the policy a waste of time.

While well-drafted policies are likely to have an effect on the conscientious employee, they still do not address two key risks facing the organisation:

- ☞ Individuals or groups who *deliberately* want to misuse resources
- ☞ *Accidental* security breaches committed by unwitting users

A recent survey of 163 Fortune 1000 companies found that roughly 70 percent of all reported security breaches were due to insiders.

Ponemon Institute

What one sees when one reviews policies that organisations rely on to manage risk is a clear preoccupation with employee internet and email misuse.

These are the ways in which employees use the organisations network to communicate with third parties. Conventional wisdom has it that this is where there is the greatest exposure to the risks mentioned above.

However using policy to help manage risk will be effective only if :

- 👉 policy content focuses on the areas where the risk is highest and
- 👉 policy is enforced without disruption to core business (employees and non-employees alike)

2.4 Not all policy breaches are deliberate

Without doubt, the vast majority of employees in an organisation are trustworthy individuals who are not intent on harming their employer. However, nobody is immune from making mistakes or having accidents. The problem with the use of 'lifestyle' devices is that they fall outside corporate control and can become infected and carry a malicious payload which can be transferred to a corporate network without the user even being aware.

No matter how trusted an employee is the risk is still present.

2.5 But some are...

Malicious activity can come in different flavours, ranging from an underperforming Salesman taking a prospect list to a new competitive employer to an opportunist (such as a contractor) seeing valuable information as being accessible and unprotected.

However, an even more worrying situation is that the first cases are beginning to emerge of employees who specifically obtain jobs in sensitive positions in order to steal confidential information as part of an organised crime syndicate.

Their task is made very significantly more straight forward by the ability to take vast amounts of information in a single go via an item which is commonly available, easy to conceal and even if discovered would arise little or no suspicion.

77% of large networks contain highly-confidential information. 65% of large businesses would face significant disruption if data was corrupted.

Information Security Breaches Survey 2004

3. Re-focusing on areas of unaddressed risk

Through investments in anti-virus and content filtering solutions, many organisations have successfully combated the risk of dangerous or inappropriate information entering or leaving the enterprise through the corporate network via email or internet. But the new breed of lifestyle technology devices have opened up a dangerous 'back door' onto the network, enabling anyone with computer access to deliberately or accidentally remove sensitive information or introduce security threats.

Characterised by their small physical size, yet significant data capacity, these devices include:

USB drives	The most obvious example is the advent of the USB storage device commonly known as a "memory stick" or "thumb drive" - a device with a massively superior memory capacity capable of storing in its most sophisticated form many hundreds of thousands of documents all in an item that will fit in a jacket pocket. Up to 2 GB capacity for less than \$150.
Media Players	While media players such as Apple's iPod are sold with a specific purpose in mind - namely the storage and reproduction of music - they can be used to hold all manner of electronic data and often have a huge memory capacity many times that of an average PC just a few years ago.
PDA's	PDA's are now routine in many workplaces and have relatively large computing power with associated memory capability. Even mobile phones are now supplied with substantial memory capacity far in excess of that needed to fulfil their primary purpose. All of these devices share a common link which is the speed and ease with which they can interface with a PC and beyond that organisation's entire network.
CDs & DVDs	With a storage capacity of up to 800 MB for CDs and 4.7 GB for DVDs, these media present a far more potent risk than their older floppy disk counterparts. And with the majority of PCs now fitted with CD or DVD writers as standard, it's never been easier for employees or opportunists to remove vast amounts of data.
Floppies	Only 1.44 MB data capacity, but still enough to remove confidential files, employee records or tender documents.
Mobile Phones	Many mobile phones now feature contact and diary applications which can be synchronised with their PC-based counterparts. A growing number of these phones also support other file formats, which make them a perfect 'undercover' storage medium for those wishing to avoid suspicion.
Wireless Ports	Many laptops now feature bluetooth, IRDA and Wi-Fi connectors as standard. Data transfer has never been so easy.

The common link between all the devices listed above is the speed and ease with which they can interface with a PC and the organisation's network beyond. As the next section shows, the risk presented by these technologies to the integrity of the network is enormous.

A recent study showed that 70% of staff have stolen key information from their workplace – with at least 72% of offenders having no ethical issues with helping themselves to information that would benefit them in their new job.

BBC News, 'Workplace data theft runs rampant'



2,500 songs, or your prospect database?



Great gadget, or massive security risk?



Personal diary, or company employee records?

4. What are the risks?

While many of the devices outlined in section two might appear innocent – and were more than likely designed with entirely legitimate uses in mind – the reality is that they present a number of security risks for the organisation.

Here are just a couple of examples:

4.1 iPods and media players

Employers are reporting a steady rise in the number of media player devices being brought into the workplace. While some staff might simply want to listen to the music already stored on the player, increasingly employees are retrieving songs already downloaded to their PCs using the company's high-speed internet connections. This causes a number of issues for the employer, not least among which are the vicarious liability associated with copyright infringement (even paid-for music downloads are usually the property of the employee, not the employer whose networks they sit on) and the use of corporate resources to store large amounts of personal data.

And if that wasn't serious enough, it pales when compared to a risk that something more than music is being transferred from the employer's system. Using a Firewire connection, an iPod can easily download around 6GB of data files from your network in just one minute.

4.2 USB sticks and memory cards

While an employer may at least notice the presence of a media player, they are much less likely to spot someone with a memory card or USB stick. But with a data capacity of up to 2GB and no specialist software required to connect the device to a PC, USB sticks and memory cards present perhaps the greatest risks to the integrity of the network. With costs starting from as little as £5, accessibility has never been easier.

4.3 PDAs and mobile phones

PDAs and mobile phones are now commonplace, with style and novelty often exceeding practical use. Around most offices these devices rarely warrant a second glance. Yet in the hands of a disgruntled employee or opportunistic contractor, these present a highly effective means of copy sensitive from the network.

Whether by accident or design the introduction of any of these devices to a network also carries the risk of virus or other malicious code. Often the other system to which the device will be connected is the owner's home PC. In contrast to the employer's system which will have a range of software in place to detect and prevent virus' home systems often have little or nothing in place.

4.4 Categorising risks

Loss of Confidential Information

The unauthorised release of confidential information can present huge problems for businesses ranging from a loss of competitive advantage to a loss of reputation or brand damage or even to court actions. Industrial espionage is increasing generally. The most common example occurs when employees move jobs and involve themselves in what they feel to be at the time to be legitimate exercise in taking material (including trade secrets and customer databased) from their current employer to their new employer.

Intellectual Property Rights Infringement

The vast majority of content accessed by employees, whether it is held locally or on the internet, is subject to some form of intellectual property or copyright law. On one hand, this should give good reason for organisations to stop sensitive information leaving their networks – and on the other, they should guard against the unauthorised transfer of such content to and from their networks, as they lay themselves open to a significant risk of prosecution by a third party laying claim to the copyright.

Corruption of Data and Systems

Despite an overwhelming majority of organizations having an anti-virus solution in place, 68% of businesses suffered at least one virus infection in 2004, with two-thirds of these reporting a virus outbreak as their 'worst incident' of the year (source: DTI, UK). Indeed, the disruption that can be caused by the introduction of viruses and malicious code are well documented.

While most organisations have taken steps to protect themselves from the number one method of virus propagation – email and internet downloads – many are still susceptible to malicious code being introduced directly through a PC on the network.

And it's set to get worse. Anti-Virus vendor, MessageLabs, expects to see an increase in 2005 of "Trojans and other malicious code designed to specifically compromise certain organisations."

Vicarious liability

Put simply, vicarious liability means that an employer can be held responsible for negligent acts by its employees – regardless of whether their actions were specifically authorized by the employer. This means that, in addition to data loss or threat introduction, employers face a significant risk if their networks are used to transfer inappropriate content.

Breach of Privacy / Data Protection laws

With increasingly strict data protection laws now in place, lack of control over what information leaves and enters the network can lead to investigation by industry watchdogs such as the FSA and SEC, and even prosecution for company directors.

A growing plethora of legislation:

- 📄 Sarbanes Oxley
- 📄 HIPAA
- 📄 Turnbull Report
- 📄 Freedom of Information
- 📄 Data Protection Act
- 📄 Basel II

5. Establishing permissible use

Having established what the security risks around portable media devices are, it is worth reminding ourselves that there are certain situations in which you want to permit the use of these technologies. Such scenarios might include:

- ☞ Use of USB stick by authorized systems administrator to upload application patches quickly to desktops
- ☞ Diary synchronization to PDA by field based operatives
- ☞ Ability to burn CDs in the marketing department

In the vast majority of organizations, the number of 'permissible' tasks will be relatively small and unlikely to change on a regular basis.

With this in mind, policy managers would be well advised to first create a table similar to the example below, which makes it easier to establish which scenarios the policy needs to allow for:

	USB Sticks	PDA Synch	Burn CDs	Diskette Access
General Users	no	no	no	no
Dept Managers	no	YES	no	YES
Field Sales	no	YES	no	no
Finance	no	no	no	no
IT Admin	YES	no	YES	YES
Marketing	no	no	YES	no
R&D engineers	no	no	no	no

Creating a 'white list' of permissible actions allows the organization to shape its policy to accommodate legitimate actions by authorised staff while by default blocking all other transactions.

6. Revising your security policy

There is a strong case for revising existing policies to take account of the emerging threat of Lifestyle IT. A well drafted policy will reflect the risks posed by these new devices. Organisations should consider:

- 🔗 Prohibiting the use of portable data storage media and devices except with specific authority
- 🔗 Prohibiting the use of USB ports on a computer without specific authority
- 🔗 Prohibiting MP3 Players being connected to PCs
- 🔗 Restricting connection of personal PDAs to company-owned PCs
- 🔗 Prohibiting the connection of mobile phones and cameras
- 🔗 Controlling connection of non-company PCs to the corporate network
- 🔗 Improved security vetting before access to a network is given to new or temporary staff
- 🔗 Limiting the capacity of data storage devices issued by the organisation
- 🔗 Amend definitions of 'misconduct' within appropriate HR policies to reflect the new issues facing organisations as a result of these lifestyle devices

"Some of this year's hottest gifts, especially for teens, are those tiny, portable digital music players such as the pack-leading Apple iPod and competitors like Creative Zen Micro and Rio... But technology security experts warn that many of this holiday season's millions of newbie MP3 player owners don't know what dangers lurk behind some music."

'Trouble can be downloaded along with music', Washington Post, December 28 2004

Any policy issued by an organisation should be compatible with prevailing applicable laws, regulatory requirements and best practice. As such, research is a vital stage in the preparation of policy; the internet, trade publications and third party professionals can all assist in setting the parameters for what should and should not be in a policy.

The requirements of the organisation itself will also have to be considered and will usually be easy to establish. The final decision as to what goes into a policy is a matter of commercial judgement as in reality a policy which sets out to be too comprehensive will fail as a useful document.

When drafting policy it is important to reflect a consistent tone and culture expected within the company and as such, use of appropriate language is critical to convey both the spirit and intent of the policy. Above all else the creator of policies should strive to use plain language at all times and should shy from legal and needless jargon. The policy needs to be capable of being understood by all who are affected by it and should be unambiguous.

Before a policy is deployed for the first time the organisation should consider whether a consultation process needs to be undertaken either directly with those affected or via a staff consultative body.

7. Deploying and communicating the policy

A deployment mechanism should be adopted that includes targeting the right policies to the right people. Some policies are truly applicable to all communities within an organisation but many more will apply to only some.

To avoid wasting time and reducing the impact of a relevant policy when it is deployed care needs to be taken in this area. The organisation should consider the best deployment mechanism for each policy individually.

Where a policy requires the employee to take action (e.g. “not download business data files to portable storage devices”), it is not enough to simply write the policy and place it in the employee handbook or upload it to the company intranet.

If an organisation wants to ensure that it has met its obligation to properly inform employees of the applicable policies, it must take steps to ensure that the policy is properly deployed.

Ideally, this should be a two fold process, it includes obtaining evidence that the employees agree to abide by the policy and moreover and beyond this it includes takings steps to establish that there is a real understanding of policy.

Finally those charged with deploying policy need to be in a position to readily generate reports on the deployment process. As a basic minimum management reports to show compliance at a glance are valuable to those leading the organisation, an ability to share reports to the interested parties such as partners, customers, regulatory bodies, to demonstrate compliance can be a useful tool, to win work or deal with unwelcome scrutiny.

Moving down to the detailed level it is necessary to be able to identify a particular individual or group to whom a policy has been deployed and ascertain whether and when they agreed to abide by the policy and exactly what was included in that agreement.

Checklist

- ☞ Policy must be read by all affected employees
- ☞ Policy must be understood, and agreed to, by relevant employees
- ☞ Employees should be required to sign-up to the policy
- ☞ Employers should keep a record of policy, formal changes and employee acceptance
- ☞ Policy should be periodically re-presented to maintain employee awareness

“Unmanaged mobile devices represent one of the most serious and often overlooked security threats to the enterprise.”

David Friedlander, Forrester Research

8. Enforcing the policy

While a clear, well-communicated policy is an essential part of any organisation's IT security strategy, firms cannot rely solely on goodwill to shape the actions of all employees. What's needed is a means to enforce the security policy.

IT heads need to be able to directly reflect their organisation's security policy with a network-wide solution that supports 'permissible uses' of media devices (see Section 4) but blocks unauthorised connections.

Unfortunately, IT managers cannot turn to their standard Windows installations for this level and granularity of security. However, there is a solution...

8.1 Introducing DeviceWall®

DeviceWall from Centennial Software allows organisations to close the security 'back door' preventing the unauthorised transfer of content to and from corporate PCs using removable media devices, such as music players, USB sticks, PDAs, memory cards, CDs and even wireless devices.

DeviceWall allows the legitimate use of approved devices (preferably, but not exclusively, provided by the organisation) by authorized staff – ensuring that business productivity is not affected – while actively guarding against the removal of data or the introduction of risks to the network by unauthorised parties.

8.2 Using DeviceWall to support permissible usage tables

DeviceWall makes it easy to establish flexible access controls based on user groups, business units or individual employees. This makes it simple for administrators to mirror established permissible uses (for example, you may allow field sales operative to access PDAs, but no-one else) based on the legitimate needs of users.

Using DeviceWall's simple Control Centre interface, the administrator simply browses the Active Directory or network domains to select which users should be allowed access to particular devices.

Active Directory

For organisations that have already made the investment in Active Directory, DeviceWall can reflect the user groups already established, making it easy to grant the appropriate permission to pre-configured groups of employees.

8.3 Temporary Access Requirements

To cater for those exceptional occasions where an employee will have a legitimate request to be temporarily exempt from a policy (e.g. a sales representative on-site with a customer needs to take information from a USB drive), DeviceWall supports authorised temporary policy over-rides for both online and offline users.

For users connected to the network, this can simply be done through an updated policy sent immediately to the specific user's PC. For offline users who have no access to the internet, a different solution is required. DeviceWall features a temporary access mechanism which enables administrators to remotely grant access to a specific device until the end of the current Windows session through a verbal key exchange process.

8.4 Deployment

DeviceWall can be quickly and easily deployed by a single administrator from a central server to the entire local or global network. Centennial Software's advanced deployment technology means DeviceWall can be automatically deployed across LAN and WAN network with no 3rd party tools required.

8.5 DeviceWall at Work – example scenarios


With its ability to protect the network from unauthorised activity - while still allowing legitimate users to go about their business – DeviceWall is the ideal real-world solution for maintaining network integrity:

 **Scenario 1 – “DeviceWall stopped me copying confidential files”**

Contractor Jonathan doesn't mind how he makes his money, either from the companies he works for or the people who would pay for the information he has access to. But his attempts to copy customer account information from an unmanned PC were thwarted by DeviceWall, which blocked access to his PDA.

 **Scenario 2 - “I nearly introduced a virus onto my PC by accident”**

Catherine borrowed a USB stick from a friend which she believed had holiday photos on. What she didn't know was that the device was also carrying a virus which could have caused havoc on the network. DeviceWall blocked access to the USB drive, preventing costly damage to files.

 **Scenario 3- “I was offsite and needed urgent access to my CD drive”**

At a meeting with an important client, Joe needed to copy files to a CD. While Joe did not normally have privileges to write CDs, his manager agreed that this was a special case and an administrator was able to allow Joe temporary access to write the CD, keeping the client happy.

9. Conclusion / Summary

The proliferation of small portable media and storage devices has changed the security threat facing most organisations today. Perimeter security mechanisms have largely addressed the risks associated with external attacks or internet and email connections being used to transport unauthorised content into and out of the enterprise – but these technologies have no ability to stop such transactions at the desktop or laptop.

DeviceWall is the simple way to dramatically reduce the risks associated with content entering or leaving the network through corporate PCs. By denying access to unauthorised portable devices, DeviceWall stops both accidental and deliberate security breaches.

When dealing with Lifestyle IT, remember these three steps:

- 👉 Define permissible use
- 👉 Set & communicate the policy
- 👉 Enforce policy with DeviceWall

Visit www.devicewall.com to find out more about DeviceWall or contact us on 01793 344052.

Centennial Offices:

Head Office, EMEA

Centennial Software Ltd
WindRiver House
10 Viscount Way
Swindon
SN3 4NT
United Kingdom

Telephone: +44 (0)1793 836200
Facsimile: +44(0)1793 836201
Email: emea@centennial-software.com

Americas

Centennial Software
4380 SW Macadam Ave
Suite 245
Portland
OR 97239
United States of America

Telephone: +1 503-238-7455
Facsimile: +1 503-238-7473
Support: +1 503-238-7455
Email: americas@centennial-software.com

Germany

Centennial Software
Am Rodland 33a
D - 63674 Allentstadt
Deutschland

Telefon: +49 (0) 6047 6281
Telefax: +49 (0) 6047 6283
Email: emea@centennial-software.com

Asia Pacific

Centennial Australia
Level 4
201 Miller Street
North Sydney
NSW 2060
Australia

Telephone: +61 2 9973 4151
Facsimile: +61 2 9918 5992
Email: apac@centennial-software.com

10. Appendices

A1. Quick Reference Checklists:

When revising your security policy to include portable media devices, these are the key questions you will need to answer:

Writing policy

- ☞ What are the legitimate needs for employees to use removable media devices?
- ☞ Does your policy address all the key threats (music players, USB sticks, PDAs etc.)?
- ☞ Have you used plain language that will be understood by all employees?
- ☞ Have you outlined the disciplinary consequences of failure to follow policy?

Deploying policy

- ☞ How will the policy be seen by all affected employees?
- ☞ What practices are in place to handle temporary staff and contractors?
- ☞ How are employees required to demonstrate an understanding of the policy?
- ☞ How will you record when employees formally signed-up to the policy?
- ☞ When do you plan to update and re-deploy the policy?

Enforcing policy

- ☞ Can you control what removable media devices can be connected to your network?
- ☞ Are you able to grant permissions to certain devices automatically depending on user group membership?
- ☞ Do you have a process / mechanism to allow one-off access to normally restricted devices?

A2. Sample Acceptable Use Policy

The sample policy below has been drafted with the assistance of specialist IT and employment law firm, Cater Leydon Millard. Certain areas of this policy, which are especially important when considering the threat of portable devices, have been colour-coded in red.

While this draft document is designed to help you understand how your computer use policies need to address the various risks facing your organisation, it is not intended to be definitive statement. Legal advice should always be sought before taking action in reliance on any information contained in this guide or in the preparation of a policy governing the use of an organisations IT network.

Draft Policy

Introduction and Scope

1. This Policy relates to the use and monitoring of all of the Company's IT and communication systems, including telephones, mobile telephones, facsimile machines, computers (including laptops and personal organisers), email, the internet, the intranet and the extranet.
2. The Company provides the IT and communication systems for business purposes and the use of these systems at all times is subject to this policy. Breach of this Policy in your use of the Company's IT and communication systems will be considered a disciplinary issue.
3. This Policy applies to all employees, contractors and agents ("staff") who use the Company's IT and communication systems.

Email

4. Email correspondence is not private. Emails can be easily intercepted, copied, forwarded and stored without the original sender's knowledge. You must take into account the fact that any email you send may be read by a person other than your intended recipient.
5. Any attachments which contain important or confidential material should be encrypted or password protected.
6. All messages and files are automatically scanned for viruses before being introduced into the network, but this does not provide a complete guarantee of protection. All employees have an obligation to be cautious when opening emails and attachments to emails from unknown sources. If you have any doubts about opening an email or attachment, speak to the IT Department first.
7. Contracts can be entered into by email in the same way as they are by letter or on the telephone. You must at all times take care to ensure that you do not inadvertently enter into contracts which bind the Company by email, and you should be aware that contracts must only be entered into in accordance with the normal procedures.
8. You must not under any circumstances send messages or attachments whether within the Company or outside the Company which are;
 - a. Abusive including the use of foul language
 - b. malicious
 - c. discriminatory in any sense (e.g. sex, sexual orientation, age, race, religion, gender or disability)
 - d. defamatory about any other person or organisation
 - e. bullying or intimidating in content
 - f. sensitive or confidential

Acceptable Use Policy cont'd

If you receive any such messages from outside the Company you must delete them and must not forward them either within or outside the company.

Sending emails of the type described above is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct.

Internet

9. The Company has put technical measures in place to prevent access to internet web sites which contain explicit, illegal or other inappropriate materials. If you need to access a site which contains such materials for the purposes of your job you must obtain the express permission of the Company.

10. Much of the information that appears on the internet is protected by copyright. Unauthorised copying or modifying of copyright protected material, including software, breaches copyright law. Therefore, downloading software or copyright protected information is not permitted, as it may make you and/or the Company liable to legal action.

Confidentiality

11. You must not use the Company's IT and communications systems whether alone or in conjunction with any other device to make an unauthorised disclosure or copy of confidential information belonging to the Company.

12. The unauthorised disclosure or copying of information belonging to the Company is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct

13. Such confidential information shall include without limitation details of:-

- a. Business contacts, associates, lists of customers and suppliers and details of contracts with them
- b. Identities of potential customers and suppliers
- c. Sales, expenditure levels and buying and pricing policies including details of percentage mark-up of profit and discounts
- d. Proposals, plans or specifications for the development of the existing products and of new products to be sold or developed
- e. accounts, trading statements, statistical information and other financial reports
- f. Corporate and marketing strategy, business development plans, sales reports and research results and forecasts
- g. Details of the employees and officers of the Company and of the remuneration and other benefits paid to them
- h. Presentations, tenders, projects, joint ventures or acquisitions and developments contemplated, offered or undertaken by the Company

Monitoring and Data Protection

14. In order to protect the interests of the Company and to maintain the effectiveness, integrity and security of the Company's network, the Company has tools in place to monitor and intercept telephone and email communication and internet use by staff.

Acceptable Use Policy cont'd

15. Monitoring is undertaken using the following automatic procedures:

- a. Automatic checking of emails and attachments for viruses.
- b. Automatic checking of emails for multimedia attachments and offensive words.
- c. Automatic checking of disks, CDs and internet sites for viruses
- d. Automatic measures in place to prevent software from being downloaded to, installed on or deleted from the Company's computers
- e. Automatic blocking and recording access to certain files and pages on the internet
- f. Automatic Recording of telephone and mobile telephone call destination numbers
- g. Automatic blocking of access to premium rate telephone lines
- h. Automatic blocking of the connection of unauthorised devices to the network

16. Monitoring of the content of emails, internet use or telephone calls is not routinely carried out but may be carried out in some situations. For example (this is not an exhaustive list):

- a. Where the Company has reasonable grounds to believe a staff member is breaching this or any other policy of the Company
- b. Where there is a suspected breach of contract or a serious under-performance
- c. For the purpose of assisting in the investigation of wrongful acts
- d. To comply with any legal obligations
- e. For the purpose of defending or prosecuting any legal action brought against the Company

17. You should not expect that your personal use of the Company's IT and communication systems to remain private.

18. The holding, processing and disclosure of personal data in electronic form is regulated by the provisions of data protection legislation. Personal information relating to a living individual who can be identified from that information should not be sent by mail unless proper checks have been made to ensure that this will not involve any breach of that legislation.

19. You must also comply with the Company's Protection Policy.

Security

20. Employee access to the Company's IT and communication systems is subject to satisfactory security checks being carried out in the reasonable discretion of the Company.

21. If you are provided with a portable computer, mobile phone, personal organiser and/or any related or similar equipment, you must ensure its security at all times. You must in particular

- a. Never leave computer equipment including discs, CDs and DVDs in an unattended vehicle, or unattended in public
- b. Always lock mobile equipment when not in use so that it cannot be used without entering your log-on ID
- c. Keep your passwords confidential and the IT system will force you to change them regularly
- d. Lock the terminal if you leave a terminal unattended so that it cannot be used without entering your log-on ID in order to prevent unauthorised users using it in your absence

Acceptable Use Policy cont'd

22. If your computer equipment is lost or stolen you must report the incident to the police immediately, and notify your line manager as soon as possible. The incident will be fully investigated, and may be treated as a disciplinary issue if you have failed to take adequate steps to safeguard the security of equipment in your possession.

23. You must not attempt to gain access to any part of the network to which you are not permitted access.

Computer and other equipment not provided by the Company

24. You must not connect or attempt to connect any device to the network without express authority from the IT Department and you should be aware that the Company has in place automatic measures to prevent this.

25. In particular you should not attempt to connect any of the following devices to the Company's network:

- a. A file or information storage device
- b. A mobile phone not issued by the Company
- c. An MP3 Player or similar device
- d. A gaming device

26. A breach of the prohibition contained on connecting devices to the Company's network is likely to be treated as a disciplinary offence and could give rise to a dismissal for gross misconduct.

Personal Use

27. A limited amount of personal use of the Company's systems is permitted subject to the following rules:

- a. Work on the Company's business must always take priority over your personal use of the Company's systems
- b. Any personal use must not delay or interfere with the proper performance of the duties of any member of staff
- c. All personal email messages must make it clear that they are sent in a personal capacity and not on behalf of the Company and must include in the subject field a statement that the email is "Private"
- d. Where you are in receipt of personal emails you should advise the sender that these may be monitored
- e. All personal emails should be deleted as soon as read or sent
- f. You may not subscribe to any non-job related Internet service or access any web based personal email accounts using the Company's systems
- g. You may not use the Company's systems to transfer , store or download information and files for your personal use including (but not limited to) MP3, AVI, WMV files and other similar formats

If your personal use exceeds an acceptable level in the reasonable opinion of the Company or you do not comply with these rules your access to the system may be curtailed and you may be subject to disciplinary action.

Consequences of a Breach of this Policy

28. Breach of this Policy in your use of the Company's IT and communication systems will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:

Acceptable Use Policy cont'd

- a. Excessive visiting of non-job related internet sites during your normal working day
- b. Introducing a virus to the computer system by inserting a disk, CD or DVD into a Company computer without running a virus check, via email or from downloading an Internet file
- c. Misuse of the computer system which results in any claim being made against the Company
- d. Accessing pornography or any other illegal material on the Internet and/or circulating it
- e. Unauthorised copying or modifying of copyright material
- f. Unauthorised downloading of software or files
- g. The connection of an unauthorised device to the network
- h. Use of the Internet for criminal activity

In less serious cases you may have access to the internet from your computer removed or other disciplinary action taken against you short of dismissal.

End of Policy