Accounting Package Selection

Selecting the right accounting package can be difficult, particularly as there are so many packages on the market. Price and functionality vary so widely as to make objective comparisons very difficult without spending a number of days on the selection process. The availability of internet (cloud-based) accounting packages has complicated selection.

We have set out below some areas you should consider when making your selection.

Determining your requirements

A decision is required as to what level of complexity is required.

At the most basic level, you need to decide whether you just want something to replace the cash-book, to handle receipts and payments, or perhaps a more sophisticated ledger-based system to produce quotes, VAT returns, and monthly accounts would be more appropriate.

You may decide that you need a highly sophisticated system which, as well as doing all of the above, can also handle stock control and job costing and which also integrates with a web site.

On-line or in house?

The next key decision is whether you want to run your accounting functions in house, or over the internet using a web-based provider. There are advantages and disadvantages either way. For example, an online solution will involve a recurring monthly fee for the service whereas an in house solution will involve a one-off purchase price and then annual licence and upgrade fees. Also to consider with an online solution is how secure is the data and can it be retrieved in the event the provider "disappears" or goes into administration/ receivership.

The growing business

Think about what the business might be doing in say, 12-18 months' time:

- will it be going through rapid growth or a change in direction, and need more up to date and more accurate financial information, such as profitability at department or cost centre level?
- will transaction volumes be rising steeply?
- will you want to be able to connect your products to your web site and process orders and payments on-line?

Market sector

Your business may be in a specialist market sector for which there are tailor made systems already available. Talk to us as we have experience of your type of business. Talk to your trade association - they may already produce information to help you, and they may hold events and seminars on this issue.

Cost

Cost should not be a primary constraint, as you tend to get what you pay for. If you are only willing to spend, say £100, the system will be unlikely to meet all of your needs. This in turn may constrain the way the business trades, and subsequently turn out to be a hindrance to expansion. It may also mean that more expenditure and upheaval is required if you need to upgrade to a more expensive system in the future.

Some systems are available in modules. Examples of modules are a sales ledger module and an invoicing order module.

If you are purchasing a modular system you won't need to purchase every module at the outset. You will need the core ledgers to start with (sales, purchases and nominal/general ledgers) and you can then add any additional modules later. In this way the costs can be spread out over a period.

Training

Training is vital for the staff that will be using the system on a day to day basis. Do not assume that an experienced user would not benefit from training.

We may be able to provide training for you or help you find appropriate training.

Your detailed requirements

A list of your detailed requirements would be useful when comparing packages. The following pointers need to be considered in the context of your business.

General points

- What is the operating system for your computer network? (There is less of a choice of accounting packages if using a non-Windows platform).
- How many users will require access (now or in the future)?
- What volume of transactions will you be processing and can the software handle this?
- Can the system produce VAT returns and, if you are on a special VAT scheme, can it cope with this?
- Can orders and payments be taken over the internet and downloaded to the accounting system?

Continued >>>

- Will the system let you export data to other packages such as spreadsheets and word processing packages?

Your specialist processing requirements

Here is a sample list – you will need to add your own special requirements depending on the nature of your business:

- retentions
- deposits/subscriptions/donations
- discounts – quantity and value discounts
- part-payments/part-receipts/part-delivery
- foreign currency customers and suppliers, and foreign currency fluctuations
- processing adjustments such as bounced cheques, bad debt write-offs, refunds etc
- direct debits/standing orders (receipts and payments) and multiple debit/credit card accounts
- accruals and prepayments
- loans, grants and mortgages and any special payment terms
- component stocks and bill of materials
- mixing of service and stock items on an invoice and as separate stock records
- payments to suppliers electronically (via BACS)
- HP agreements
- label and mail shot capabilities for customers/suppliers
- ability to create XML formatted transactions (to facilitate electronic transmission to other systems)
- debt factoring/financing (may require specific work rounds)
- data import and data export requirements

Your information and reporting requirements

You need to determine what kind of management and user information is required from the system.

A sample list might include:

- financial reports – trial balance, profit and loss, balance sheet, cash flow and turnover reports
- key ratios and other business metrics
- work in progress and profit/loss on job or contract
- profit/loss by department, or by cost centre or other levels of analysis
- customer/supplier balances and aged debtors/aged creditors
- statements and invoices
- actual v budget reports

Other points

- How does the system cope if you need to amend a transaction?
- Is there a full audit trail (including details of modified transactions)?
- Does the system produce the information in an acceptable form to you and us (as your accountant) in order to complete all statutory and regulatory financial year-end and fiscal year-end tasks?
- Does the system enable statutory online filing (VAT returns, EC Sales List returns for example)
- Are there adequate security routines to prevent employees exceeding their level of processing authority (ie being able to restrict access on an individual user basis)?

The final choice

- Narrow the selection down to the package(s) that matches your needs most closely.
- If the potential user(s) of the system have not so far been involved, now is the time to get them involved.
- Get an evaluation copy if possible (some software vendors offer a free 30-day trial), and also go and see the system in action at a business similar to yours.

Having performed an objective review up until now, the final choice may be more subjective. It will probably be down to look and feel at the end of the day!

Implementation

Whilst the beginning of the financial year is the most logical time to start, this may not be a particularly convenient time for the accounts staff.

You may wish to discuss the timing with us, as we can help in drawing up a list of opening transactions and the opening trial balance at the appropriate time.

Other issues to think about at this stage are:

- staff training
- customer/supplier/nominal and cost centre/stock/job costing codes
- ordering any pre-printed stationery
- creating records and posting opening transactions (if you already have a system in place it may be possible to import some or all of this data)
- developing periodic processing, authorisation and verification routines
- backup procedures for the accounting data files
- long-term retention of accounting records (minimum of 6 years).

You may find it useful at this stage to refer to our factsheet on Data security.

How we can help

We are here to help you with any of the steps involved in choosing and implementing an accounting package. Please contact us for further advice.

Data Security - Access

Many businesses are now completely reliant on the data stored on their Network Servers, PCs, laptops, mobile devices and cloud service providers or internet service providers. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems with respect to access controls, and to ensure compliance with Principle 7 of the Data Protection Act. This states that -

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Access security

Good access controls to the computers and the network minimise the risks of data theft or misuse.

Access controls can be divided into two main areas:

- Physical access – controls over who can enter the premises and who can access personal data
- Logical access – controls to ensure employees only have access to the appropriate software, data and devices necessary to perform their particular role.

Physical access

As well as having physical access controls such as locks, alarms, security lighting and CCTV there are other considerations such as how access to the premises is controlled.

Visitors should not be allowed to roam unless under strict supervision.

Ensure that computer screens are not visible from the outside.

Use network policies to ensure that workstations and/or mobile devices are locked when they are unattended or not being used.

Ensure that if a mobile device is lost there are ways to immobilise the device remotely.

Mobile devices being small are high risk items and so sensitive data should always be encrypted and access controlled via a pin number or password.

It may be necessary to disable or restrict access to USB devices and Optical readers and writers.

Finally, information on hard-copy should be disposed of securely.

Logical access

Logical access techniques should be employed to ensure that personnel do not have more access than is necessary for them to perform their role.

Sensitive data should be encrypted and access to this data controlled via network security and user profiles.

Access to certain applications and certain folders may also need to be restricted on a user by user basis.

Finally, it may be necessary to lock down certain devices on certain machines.

Passwords

It is accepted, universally, that a password policy consisting of a username and password is good practice.

These help identify a user on the network and enable the appropriate permissions to be assigned.

Passwords to be effective, however, should:

- be relatively long (i.e. 8 characters or more)
- contain a mixture of alpha, numeric and other characters (such as & ^ ")
- be changed regularly through automatic password renewal options
- be removed or changed when an employee leaves
- be used on individual files such as spreadsheets or word processed documents which contain personal information

and **should NOT**

- be a blanket password (i.e. the same for all applications or for all users)
- be written on 'post it' notes which are stuck on the keyboard or screen
- consist of common words or phrases, or the company name.

How we can help

We can provide help in the following areas:

- defining and documenting security and logical access procedures
- performing a security/information audit
- training staff in security principles and procedures.

Please contact us if you would like any help in any of these areas.

Data Security - Backup

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices and on data stored in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems and data.

Data backup is an essential security procedure and needs to be undertaken on a regular basis. A business should view the taking of regular backups as a form of insurance policy. There are a number of points to consider.

Systems and Applications Software Installation media

Ideally, once software has been installed, the original media (unless the software was downloaded) should be stored securely off-site.

Data file locations

In a network environment some data files might be stored on the server and other data files stored on local drives. In which case separate backups may be required for both the server and one or more PCs.

Ideally, a network solution should be provided which ensures that all data is re-copied back to the server from local drives.

Backup strategy and frequency

There is likely to be a need for two parallel backup procedures; one to cover a complete systems backup of the server(s) and another to incrementally (or differentially) backup data files which have been updated since the previous backup.

The most common backup cycle is the grandfather, father, son method. With this, there is a cycle of 4 daily backups, 4/5 weekly backups and 12 monthly backups.

Remember that some data has to be preserved for many years – for example accounting records need to be kept for a minimum of 6 years.

Backup media can be re-used many times, but they do not have a finite life and will need replacing after 2-10 years depending on quality and number of times used. Some additional points are made on this issue in the section on backup media degradation.

Backup responsibilities

Someone should be given responsibility for the backup procedures. This person needs to be able to:

- regularly ensure that all data files (server and local) are incorporated in the backup cycle(s)
- adapt the backup criteria as new applications and data files are added
- modify the backup schedule as required
- interpret backup logs and react to any errors notified
- restore data if files are accidentally deleted or become corrupt
- regularly test that data can be restored, from backup media and
- maintain a regular log of backups and where the backup media are stored.

Applications backup routines

Many accounting and payroll applications have their own backup routines. It is a good idea to use these on a regular basis (as well as conventional server backups), and always just before critical update routines. These backup data files should be stored on the server drive so that they are backed up.

Local PCs

Certain users will have applications data files exclusively on their local drives (such as payroll data for example) and these will require their own regular backup regime, which as mentioned in the previous paragraph may consist of a combination of backing up to media and backing up to the server.

Backup media

Selecting the right media to use depends on budget, how much data there is and the networking operating software. External hard disks provide a good backup solution, and optical storage such as CD/DVD, or Blu-Ray may also be considered as a cheaper alternative, but capacity and life may be limited. If an external service provider is used, or perhaps a cloud option, they should have their own backup regime – but don't totally rely on this.

Backup retention

Backups should be stored in a variety of both on-site and off-site locations. On-site backups are easily accessible when data has to be restored quickly, but are at risk from either fire or other disaster.

A large number of businesses use an on-site safe, however, this will be useless if it's buried under tons of rubble, or, if the premises otherwise become inaccessible.

Off-site backups have the advantage that they can be recovered in an emergency, but

a) they still need to be stored securely and

b) need to be reasonably accessible.

Continued >>>

Finally, certain type of records, such as accounting records for example, need to be kept for a minimum period of time (i.e. 6 years) and this must be borne in mind when developing the data backup strategy (also see below regarding degradation).

Backup media degradation/decomposition

Backup media degrades and the data stored on them decomposes over a period of time.

Optical media such as CD/DVD and Blu-Ray are particularly sensitive to light (photosensitive), so ensure that they are stored in a dark environment. They are also prone to damage caused by writing on them with a pen. Finally, this type of media is not designed for long-term storage - lasting possibly as little as 2 years.

Backups should be checked on a regular basis for signs of digital decomposition, and tested to check that data can be successfully restored.

In-house or cloud?

Many internet service providers and third-party IT service organisations, now offer either as standard or as a chargeable extra, off-site data repositories and also complete online application solutions. The immediate appeal is that there is no need to internally support a server and its operating and applications software. However, there are a significant number of key security issues which should be covered as part of the agreement/contract. These should include the encryption level, the countries in which the data is processed and stored, data deletion and retention periods, the availability of audit trails of who is accessing the data and finally, who has ownership of the data if the provider goes into administration/ receivership.

We would always recommend therefore that if a third-party is used, that the business uses a combination of both traditional in-house backup solutions, and cloud backup services. Where data is stored in the cloud, then try to ensure that as little personal data as possible is processed and stored in this way.

How we can help

We can provide help in the following areas:

- performing a security/information audit
- drawing up a suitable backup regime
- training staff in security principles and procedures.

Please do contact us if we can be of further help.

Data Security - Data Loss Risk Reduction

Many companies are now completely reliant on the data stored on their network servers, PCs, laptops, mobile devices or in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the issues to consider when reviewing the security of your computer systems, and how to minimise the risks of data loss.

There have been many high profile incidents of data loss – where large volumes of personal information have found their way into the public domain.

Examples of this sort of information include health records, financial records and employee details.

A commercial organisation also faces the additional risk of data being lost to a competitor.

Obviously, the larger data losses from government and corporations hit the headlines.

However, any company, however large or small can suffer data loss unless sensible precautions are taken.

In the past year alone, according to research undertaken by the Department for Business Innovation & Skills some 87% of small businesses have experienced some sort of security breach.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

Small businesses were commonly subject to system failures and data corruption, with computer theft and fraud also featuring on the list of types of security breach.

Mobile devices in particular – which can run applications, link to corporate servers and can receive emails with corporate and personal data in the form of attachments, can be considered high risk. Firms may want to think about a BYOD (Bring Your Own Device) policy.

There are usually two ways in which data can go missing:

- an employee accidentally or deliberately loses a device, or discloses personal information
- the data is stolen through the physical theft of a device, or by electronic penetration.

Audit use and storage of personal data

Consider the potentially sensitive and confidential data which is stored by your business –

- staff records with date of birth, salary and bank account details, sickness/absence etc
- customer and supplier records with bank/credit card account details, pin numbers, passwords, transaction information, discounts and pricing, contracts information
- financial and performance data and business plans.

Confidential data is not always conveniently stored in a 'secure' database. Often employees need to create and circulate ad hoc reports (using spreadsheets and other documents) which are usually extracts of information stored in a database(s). This is quite often done at the expense of data security - as the database itself invariably will have access controls, but these ad hoc reports usually do not.

Find out what is happening to data and what controls are in place to prevent accidental or deliberate loss of this information.

Risk analysis and risk reduction

So the first key question is - If all or some of this data is lost who could be harmed and in what way?

When that is known, then steps to mitigate the risks of data loss must be taken.

So here are some steps which should be undertaken to reduce the risk of data loss –

- Take regular backups and store backup data off-site.
- Review the type of information which is stored on devices (such as laptops, mobiles or other media) which are used off-site. If such information contains personal and/or confidential data try to minimise or anonymise the data. Ensure that the most appropriate levels of data security and data encryption are applied to this data.
- Review the use/availability of USB, and other writable media such as Optical devices within the company and think about restricting access to these devices to authorised users only, via appropriate security settings, data encryption, and physical controls.

Continued >>>

- Ensure that company websites which process online payments have the highest levels of security. This means adopting SSL encrypted transmissions, and also testing for vulnerabilities from attacks.
- Have a procedure for dealing with sensitive information and its secure disposal once the data is no longer required.
- Train staff on their responsibilities, the data security procedures and what they should do if data goes missing.

Security breach

As well as risk reduction, it is also good practice to have procedures in place in the event a security breach occurs.

This should concentrate on four main areas –

1. A recovery plan and procedures to deal with damage limitation.
2. Recovery review process to assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen again.
3. Notification procedures – this includes not only notifying the individuals who have been, or potentially may be, affected. If the security breach involves loss of personal data, then the Information Commissioner (ICO) should be informed. There may be other regulatory bodies and other third parties, such as the police, the banks and the media who may need to be informed.
4. Post-breach – ensure that appropriate measures are put in place to prevent a similar occurrence, and update procedures and train or re-train staff accordingly.

How we can help

Please contact us if you require help in the following areas:

- performing a security/information audit
- training staff in security principles and procedures

Data Security - Data Protection Act

Many businesses are totally reliant on the data stored on their PCs, laptops, networks, mobile devices and in the cloud. Some of this data is likely to contain either personal information and/or confidential company information.

Here we look at some of the key compliance issues surrounding data protection and the Data Protection Act (the Act).

Most businesses process personal data to a greater or lesser degree. If this is the case, compliance with the Act is required unless one of the exemptions applies (see below).

Complying with the Act includes a notification process, handling data according to the principles of data protection and dealing with subject access requests.

In the UK, the Information Commissioner (ICO) is responsible for the public Data Protection Register and for enforcing the Data Protection Act.

Summary of the principles of the Data Protection Act

1. Personal data must be fairly and lawfully processed;
2. Personal data must be processed for limited purposes;
3. Personal data must be adequate and not excessive;
4. Personal data must be accurate and up to date;
5. Personal data must be kept no longer than necessary;
6. Personal data must be processed in line with the data subjects' rights;
7. Personal data must be secure;
8. Personal data must not be transferred to countries outside the European Economic Area (EEA) without adequate protection.

Exemptions

There are 5 main categories of exemption –

- organisations that process personal data only for:
  - staff administration (including payroll)
  - advertising, marketing and public relations (in connection with their own business activity) and
  - accounts and records
- some not-for-profit organisations
- organisations that process personal data only for maintaining a public register
- organisations that do not process personal information on computer and
- individuals who process personal data only for domestic purposes.

There are a number of more specific exemptions. However, most companies find the exemptions are too narrow, and opt to notify (see below).

Notification

Notification is the method by which a company's usage of personal data is added to the public Data Protection register maintained by the ICO. The process starts by completing the notification documentation (available from www.ico.gov.uk) and sending this back with the annual notification fee (currently £35 for the small business).

Notification needs to be performed annually (even if there are no changes).

N.B. Be wary of organisations who say they represent the ICO and who charge more than the standard £35 fee.

Subject access request (SAR)

Individuals have rights under the Act to find out whether you are processing their personal data, and to provide them with a copy of the data which is stored about them.

Most SARs must be responded to within 40 days.

An individual has the right to ask you to:

- correct or delete information about them, which is inaccurate;
- stop processing their personal data for direct marketing purposes; or
- stop processing their data completely or in a particular way (depending upon the circumstances)

A fee can be levied for dealing with an SAR - but only up to £10 (except for health or education records).

If a fee is levied, the access request does not have to be complied with until the fee has been received.

Continued >>>

Secondly, the Act makes it clear that the SAR must contain enough information to validate that the person making the request is the individual to whom the personal data relates. So it may be necessary and legitimate to ask for further identification from the originator of the SAR.

Data security

The Act says there should be security that is appropriate to:

- the nature of the information in question; and
- the harm that might result from its improper use, or from its accidental loss or destruction.

The Act does not define "appropriate" - but it does say that "an assessment of the appropriate security measures in a particular case should consider technological developments and the costs involved".

So, there a number of key areas to concentrate on -

Management and organisational measures

Someone in the organisation should be given overall responsibility for data security.

Staff

Staff need to understand the importance of protecting personal data; that they are familiar with the organisation's security policy; and that they put security procedures into practice.

Physical security

Technical security measures to protect computerised information are of obvious importance. However, many security incidents relate to the theft or loss of equipment, or to the disposal of old equipment and old printouts.

Computer security

As well as a comprehensive backup regime, appropriate access controls and mechanisms need to be in place. Websites, in particular, need sophisticated security measures in place.

As well as the Data Protection Act, there are various other Acts and regulations, which have a bearing on data security. These include:

- Privacy and Electronic Communications Regulations (PECR) 2003 - which cover 'Spam' and mass-marketing mail shots. Regulations under the PECR are also issued from time to time. For example, regulations on the use of cookies on websites were introduced as from 2012.
- Copyright Design and Patents Act – amended 2002 to cover software theft.

There may be other IT standards and regulations applicable to your business sector. For example, companies processing credit card transactions need to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).

How we can help

We can provide help in the following areas:

- performing a security/information audit
- training staff in security principles and procedures
- notification and/or compliance with regulations as applicable to the type of organisation.

Please do not hesitate to contact us if we can be of further assistance.

e-commerce - a Guide to Trading Online

According to the latest UK statistics, over 21m households (that's 80%) have internet access, and a large majority of these households will have used the internet to either purchase goods/services, or to search for a provider of goods/services.

As well as the domestic market, the internet provides a gateway to the international market place. Furthermore, it can be used to develop relationships with suppliers and other trading partners.

It is therefore vital that your business has an online presence.

This can be anything from a one page 'shop-front', to a complex product catalogue with an online ordering and multi-currency payment systems and a world-wide delivery mechanism.

Issues to consider

e-commerce does not have to be either expensive or complicated, but as with all aspects of business there are a number of issues which need to be considered –

- register the company name or trading name as a domain name (this will incur an annual fee)
- allocate both a start up and a recurring annual budget for the online project
- set some milestones for the website and a timeline for achieving these goals
- have a look at other websites and go through the check-out process – note what you like and dislike about these and how your customers might react
- bear in mind the needs of the disabled user
- decide whether to host the website in-house, or to use an external hosting company (ISP)
- consider the ease of being able to update website content on a regular basis
- have the website optimised to ensure that it features in popular search engines
- consider pay per click advertising options to increase ranking
- keep the site simple – and fast - visitors will not spend ages on navigation or waiting for pages to load, so this includes all elements of the website including graphics, searching the site, and the order and payment processes
- think about how the website will link to the back office accounting, invoicing and stock systems
- ensure that both the website and any on-line payment procedures have all available security measures in place to prevent fraud, hacking and denial of service threats
- enable the user to view/edit orders and to see order history and order tracking
- ensure that regular statistics on number of visitors, pages visited etc are available
- have a contingency plan to ensure that on-line trading can continue should there be a major problem.Legal requirements

Legal requirements

There are quite a few legal issues to contend with, some of these will not be relevant in all cases -

Who legally owns the website (and the content) and what happens if either the web developer/ISP ceases trading?

Compliance with relevant legislation which includes:

Companies Act 2006
E-Commerce regulations 2002
Privacy and Electronic Communications Regulations 2003
Distance Selling Regulations 2000
Data Protection Act 1998
Disability Discrimination Act 2005
Provision of Services Regulations 2009

Bear in mind that legislation and the rules and regulations incorporated within primary legislation change over time. For example, from 2012 all websites should be compliant with the regulations regarding the use of cookies.

How we can help

If you would like any further assistance please do not hesitate to contact us.

Internet and Email Access Policy

In order to protect the firm, its employees, customers and suppliers, all members of staff should be given a copy of the firm's policy regarding acceptable use of IT resources – particularly internet, email access, and data protection policies. It may also be necessary to have a separate Bring Your Own Device (BYOD) policy covering the use of personal devices and to what extent (if any) these can be connected to corporate information systems.

Any such policies should form part of the contract of employment – to the extent that any breaches of the policy could result in disciplinary action, and in some cases even dismissal.

Having an acceptable use policy not only helps protect the organisations exposure to rogue software, legal action, and loss of corporate/personal data but can also help in disputes with employees.

Email

Employees need to be wary of the content of all emails they may send. One email sent without thought as to the potential repercussions can have unintended consequences for both the employee and organisation.

Illegal material

Due to the uncensored nature of the material on the internet, there are a large number of web sites which contain offensive, obscene and illegal (in the UK) material. Employees should not access such sites.

Viruses and phishing

Innocent looking web sites and emails have been used to tempt users to download material which has been found to contain a virus, or to disclose company, or personal confidential data they would not normally impart.

Personal phones, personal headsets and use of social networks

Firms may wish to include references to the use of personal phones, personal headsets and social networking. The use of these or restrictions on the use of these will very much depend on the working environment.

A Model Policy Statement

To minimise these kinds of potential problems, all employers should consider setting out a policy statement for all employees embracing internet and email access.

A suggested policy statement is shown below which you may find useful as a starting point.

Policy and scope

The company/ firm (delete as appropriate) sees the internet and the use of email as an important business tool.

Staff are encouraged to enhance their productivity by using such tools - but only according to guidelines on their use as set out in this document.

The internet is largely unregulated and uncensored and we have a duty of care to protect the security of the company's/firms internal information, our customers, our suppliers and our employees from malevolent, obscene and illegal material.

[Monitoring - Optional paragraphs 1

With this in mind, the company (firm) reserves the right to monitor emails and internet sites visited, on an employee basis. However, this will only be performed where there is a suspicion of behaviour which breaches the company's 'email and internet access' policy.

Staff under surveillance will be informed, by management, that they are being monitored.

Covert monitoring will only be performed in exceptional circumstances and only when sanctioned by a senior officer(s) of the company/firm.]

[Monitoring - Optional paragraphs 2

With this in mind, the company/firm reserves the right to monitor email and internet traffic. However, individual users will not be identified in the monitoring process.]

It will be assumed that all staff understand and agree to the policies unless a director (partner) is notified otherwise. Any exceptions are to be appended to the employee's contract of employment and signed by a director (partner) and the employee.

All the company's/firm's resources, including computers, access to the internet and email are provided solely for business purposes.

The purpose of this policy is to ensure that you understand to what extent you may use the computer(s) owned by the company/firm for private use and the way in which access to the internet should be used within the company/firm, to comply with legal and business requirements.

This policy applies to all employees of the company/firm and failure to comply may lead to disciplinary action in line with the Disciplinary Procedure. In addition, if your conduct is unlawful or illegal you may be personally liable.

Continued >>>

General principles

A computer and internet access is provided to you to support the company's/firm's activities.

Private use of computers and the internet is permitted, subject to the restrictions contained in this policy. Any private use is expected to be in the employee's own time and is not to interfere with the person's job responsibilities. Private use must not disrupt our IT systems or harm the company/firm's reputation.

You should exercise caution in any use of the internet and should never rely on information received or downloaded without appropriate confirmation of the source.

Access to the internet and email

All/The following users have access to the internet and email from all/the following PCs…

Personal use

The internet may not be accessed for personal use during normal hours of employment. Occasional use for personal reasons is allowed outside working hours, however the restrictions set out in 'Browsing/Downloading material' (below) must be adhered to.

Personal emails may not be sent/received unless in an emergency or with prior authority.

[Optional paragraph on Personal use of mobile phones, personal headsets and social networking]

Emails and email attachments

Emails must conform to the same rules as issuing correspondence on the company's/firm's headed paper.

[Optional sentence - Emails must be authorised by either a director/ partner (or manager)].

Emails must not contain controversial statements/opinions about organisations or individuals. In particular, racial or sexual references, disparaging or potentially libellous/defamatory remarks or anything that might be construed as harassment should be avoided.

Emails must not contain offensive material.

Emails containing a virus must not knowingly be sent.

Emails coming from an unknown source must not be opened but disclosed to management (see Disclosure).

Emails sent externally, must contain the company's/ firm's disclaimer (see sample below)

Emails (sent and received) must be stored in the appropriate client files and use the same naming conventions which are used to store letters and other correspondence.

Browsing/Downloading material

Only material from bona fide business, commercial or governmental web sites should be browsed/downloaded.

No other material should be browsed/downloaded. This specifically includes games, screensavers, music/video and illegal, obscene or offensive material.

Laptops/portables and portable media devices

a Travelling with laptops/portables

Laptops are liable to be inspected by authorities particularly if travelling by air/sea/rail, both within and outside the UK. Where an employee has a company's/firm's laptop they must ensure that it does not knowingly contain illegal material.

Laptops containing corporate data should be encrypted.

b Using laptops/portables on remote connections

Company's/firm's laptops may be used for email/internet use without being connected to the corporate server. Appropriate security software to allow such access and to control viruses, should be installed.

c Using portable media devices

Portable media devices include USB memory sticks, USB pens, CDs, DVDs etc.

Where these contain confidential corporate or personal data, the data contained on these devices should be encrypted.

Disclosure

Employees have a duty to report the following to management:

- suspect emails/email attachments/web sites
- obscene/illegal material found on a PC
- persistent use of the internet for personal reasons
- persistent downloading of illegal/obscene/offensive material
- loss of corporate data or loss of machines and devices containing corporate data

Disciplinary

A breach of any of the policies is a disciplinary matter.

Illegal activities will also be reported to the relevant authorities.

Inappropriate use

Computers are a valuable resource to our business but if used inappropriately may result in severe consequences to both you and the company/firm. The company/firm is particularly at risk when you have access to the internet. The nature of the internet makes it impossible to define all inappropriate use. However you are expected to ensure that your use of computers and the internet meets the general requirements of professionalism.

Specifically, during any use of the computer or internet you must not:

- copy, upload, download or otherwise transmit commercial software or any copyrighted materials belonging to the company/ firm or other third parties
- use any software that has not been explicitly approved for use by the company/firm
- copy or download any software or electronic files without using virus protection measures approved by the company/firm

Continued >>>

- visit internet sites or download any files that contain indecent, obscene, pornographic, hateful or other objectionable materials
- make or post indecent, obscene, pornographic, hateful or otherwise objectionable remarks, proposals or materials on the internet
- reveal or publicise confidential or proprietary information (including personal data) about the company/firm, our employees, clients and business contacts.

The following activities are expressly forbidden:

- the deliberate introduction of any form of computer virus
- seeking to gain access via the internet to restricted areas of the company's/firm's computer system or another organisation's or person's computer systems or data without authorisation or other hacking activities.
- Downloading corporate information onto portable media devices (such as USB pen or CD) unless management has expressly approved this activity.
- Uploading personal/private information (for example music, films or photographs) from portable media devices (such as USB pen or CD) onto a local or network drive, unless management has expressly approved this activity.

Monitoring

At any time and without notice, we maintain the right and ability to examine any systems and inspect and review any and all data recorded in those systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by the company/firm. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.

In order to ensure compliance with this policy, the company/firm may employ monitoring software to check on the use of the internet and block access to specific websites to ensure that there are no serious breaches of the policy. We specifically reserve the right for authorised personnel to access, retrieve, read and delete any information that is created by, received or sent as a result of using the internet, to assure compliance with all our policies. Such monitoring will be used for legitimate purposes only.

Sample Disclaimer

This email and all attachments it may contain are confidential and intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of [the company/firm]. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, printing, forwarding or copying of this email is strictly prohibited.

Please contact the sender if you have received this email in error.

Companies Act 2006 emails and websites

Changes to Company law mean that, every company must now include their company registration number, place of registration and registered office address on corporate forms and documentation (this includes emails and websites).

In particular, all external emails must include this information – whether as part of the corporate signature or as part of the corporate header/footer.

How we can help

We will be more than happy to provide you with assistance in formulating an acceptable use policy, or if any additional information is required.