Simmers & Co
Chartered Accountants

[FACTSHEET]

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 and email access, as well as 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 are permitted to connect 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 organisation's exposure to rogue software, legal action, and loss of corporate/personal data, it 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 thoughtlessly can have repercussions and unintended consequences, for both the employee and organisation, such as large penalty fines and reputational damage.

Illegal material

Due to the uncensored nature of the material on the internet, there are a large number of websites that contain offensive, obscene and illegal (in the UK) material. Employees should not access such sites and attempts to block these where possible should be made by the business.

Viruses and phishing

Innocent looking websites 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 where they would not normally be imparted.

Employees should be given training to recognise the tell-tale signs of bogus emails and how to perform simple checks online before submitting data to a website.

Employees should also be told what the procedures are should they fall victim to such attacks.

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.

Model policy statement

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

A suggested policy statement is shown below, which provide a useful 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 in accordance with the guidelines 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/ firm's internal information, our customers, our suppliers and our employees from malevolent, obscene and illegal material.

Monitoring - Optional paragraphs - One

The company/firm reserves the right to monitor emails and internet sites visited by an employee. These may be performed at random or where there is a suspicion of behaviour which breaches the company's 'email and internet access' policy.

Staff will be informed by management that they may be monitored at any time, when using business systems.

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 - Two

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. It covers 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.

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 must not interfere with the person's job responsibilities. Private use must not disrupt 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 and with prior authority from a manager.

[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 and 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.

Emails sent with attachments containing any sensitive data must be encrypted and password protected. Passwords should never be sent by email. Where possible try to send this data by other means.

Browsing/downloading material

Only material from bona fide business, commercial or governmental websites 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 mitigate the risk of viruses or hacking, should be installed.

c) Using portable media devices

- Portable media devices include USB drive, CDs, DVDs etc
- Where these contain confidential corporate or personal data, the data contained on these devices should be encrypted.
- Where using portable devices, only business approved devices should be used.

Disclosure

Employees have a duty to report the following to management:

- suspect emails/email attachments/websites
- 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. However, if used inappropriately may result in severe consequences to both employees and the company/firm. The company/firm is particularly at risk when employees have access to the internet. The nature of the internet makes it impossible to define all inappropriate use. However, employees are expected to ensure that employee use of computers and the internet meets the general requirements of professionalism.

Specifically, during any use of the computer or internet employees 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
- visit internet sites or download any files that contain indecent, obscene, pornographic offensive or other objectionable materials
- make or post indecent, obscene, pornographic, offensive 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 a USB drive 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 a USB drive or CD) onto a local or network drive, unless management has expressly approved this activity
- installation of any software not pre-approved by the business.

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 generated, 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 email 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

Under company law, every company must 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.

Simmers and Co Chartered Accountants and Registered Auditors
Albany Chambers, Albany Street, Oban, Argyll PA34 4AL

Phone: 01631 562169 | Fax: 01631 565959 | Email: mail@simmers.co.uk

www.simmers.co.uk

Partners: David A McGregor | Jacqueline M Hoey