Appendix …

[NAME OF COMPANY OR FIRM][[1]](#footnote-1) Computer Use Policy

**Purpose of the Policy**

The purpose of this policy is to provide clear procedures and guidance for using e-mail, intranet and internet facilities on all our computer systems.

**Scope of the Policy**

The policy applies to all employees; fixed term contract employees; temporary employees; agency staff; and consultants and contractors who are provided with access to any of the Firm’s computer systems. Collectively these individuals are hereafter referred to as 'users'.

**Policy Statement**

It is our policy to encourage responsible use of e-mail, the intranet and the internet and thus to protect the reputation of the Firm and its employees. This policy aims to preserve the security of the Firm’s computer systems, to protect it and its employees against the threat of legal action and to encourage high standards of behaviour and conduct in relation to the use of computer systems.

We recognise the significant benefits of e-mail, intranet and internet usage and the facilities which we provide represent a considerable commitment of resources for telecommunications, networking, software and storage.

Internet, intranet and e-mail use is provided by the Firm for business-related purposes, i.e. to communicate with clients, suppliers and colleagues, to research relevant topics and to obtain useful business information. Unnecessary or unauthorised internet, intranet and e-mail use causes network and server congestion. Congestion slows other users, takes away from work time, consumes, supplies and ties up printers and other shared resources.

**General Points**

Users must not attempt to access information, computer files or computer systems for which they are not authorised as this may be an offence under the Computer Misuse Act 1990, and may constitute a serious disciplinary offence, which may lead to dismissal in serious cases

No software or files (including but not limited to screen savers, games, bitmaps, backgrounds, gifs and the like) may be downloaded via the internet, intranet or e-mail or installed onto the Firm’s network unless authorised by [person][[2]](#footnote-2). Any file which is downloaded must be scanned for viruses before it is run or accessed. Users must not use or incorporate any hardware not owned by the Firm into the Firm’s computer system without the express permission of [person], including external data hard drives or disks.

Users should always keep their computer passwords confidential.

The Data Protection Act 1998 applies to all data about living individuals by which they may be identified, such as names, personal and financial details and medical records. There are restrictions on the use and disclosure of this information, and it is a breach of the Act if the Firm does not keep such information secure. The security of personal data kept on the Firm’s computer system and its databases is therefore paramount, and users who are guilty of security breaches in this respect may be subject to disciplinary action which may result in dismissal in serious cases. The Data Protection Act 1998 can be viewed at:

<http://www.legislation.gov.uk/ukpga/1998/29/contents>

**The use of E-mail (Internal and External)**

E-mail makes a major contribution to efficient internal and external communication, but it should be used sensibly. The combination of informality and lack of inhibition with e-mail may result in the user sending or receiving pirated software or unsuitable material, or inadvertently publishing defamatory statements, disclosing the Firm’s confidential information, misleading recipients, entering into legally binding contractual obligations on behalf of the business without authorisation, subjecting users or third parties to harassment or discrimination on the grounds of their sex, race or disability, or introducing or spreading viruses across the system. To minimise these risks and to maintain the integrity of the Firm’s image and reputation, all users should adhere to the following guidance.

Users must be aware that an e-mail message is not necessarily a confidential means of communication. It is an insecure medium and content can easily be copied, forwarded and archived. Therefore e-mails should at all times be treated as a permanent written record which may be read by persons other than the addressees.

Users should never send strictly confidential messages by e-mail. Users must not expect any e-mail messages composed, received or sent on the Firm’s network, regardless of the use of passwords, to be for private viewing only. Because e-mail passes over the public internet and may be accessed by others, e-mails sent to any e-mail address outside the business are not secure. All external e-mails must have the following disclaimer attached to them; failure to attach the disclaimer is a disciplinary offence:

[……….] may monitor and read all e-mails as it is presumed that they are sent or received in connection with the business of [……….] or for business use only. [……….] also monitors e-mails for security reasons to ensure that no unauthorised disclosure of [……….]s confidential information is passed via the e-mail system.

*This e-mail and any attachments are confidential. It is intended for the recipient only. If you are not the intended recipient, any use, disclosure, distribution, printing or copying of this e-mail is unauthorised. If you have received this e-mail in error, please immediately notify the sender by replying to this e-mail and delete the e-mail from your computer.*

*The contents of any attachment to this e-mail may contain software viruses, which could damage your own computer system. While* [……….] *has taken every reasonable precaution to minimise this risk, we cannot accept liability for any damage which you sustain as a result of software viruses. You should carry out your own virus checks before opening the attachment.*

The same laws apply to e-mail as to any other written document and so e-mails should not contain any discriminatory, abusive or defamatory statements.

E-mail has the same status as a signed document. It is possible to enter into a legally binding contract by e-mail, or to make a statement which might later bind the Firm. Unless users are authorised by their manager to do so, they must not use e-mail in this way.

The Firm’s e-mail facilities are provided for business use only. Limited personal use of e-mail is acceptable provided it is for occasional social or domestic use only and does not relate to private business activities.

The use of our computer or e-mail systems for any of the following is strictly prohibited;

* drafting, sending or forwarding any e-mail which might be considered by a recipient to be offensive, defamatory, discriminatory or bullying, e.g. on the grounds of sex, sexual orientation, age, religion, race or disability or any other personal characteristic
* accessing, circulating, distributing or otherwise publishing offensive material, including pornography; ‘offensive’ means anything giving or meant or likely to give offence or insult
* circulating messages with large attachments - for example, large files, video clips or games, non-standard screen savers/wallpaper or games, or
* circulating e-mail ‘chain letters’.

To minimise the risk of virus infection users should not open e-mails from unknown sources or e-mails which have attachments which look suspicious or are from a source which does not usually send attachments. [person] should be contacted immediately and s/he will check that the attachment is free from viruses. Users must immediately comply with any instructions given by [person].

No user may use the Firm’s computer or e-mail facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Users must not infringe copyright or trademark laws when composing or forwarding e-mails or e-mail attachments - for example, users should not copy material (such as artwork) created by third parties unless the user has their express permission.

Users must not upload onto any Firm’s computer any software, whether it is licensed to the Firm or not. Any software to be installed on our systems will be dealt with by [person].

Storage of large numbers of e-mails uses up valuable memory. Where possible, e-mails which are no longer required should be deleted.

**Use of the Internet and Intranet**

Internet and intranet access is for business purposes. It is provided to enable better performance of an employee’s duties. Unless there is an express business-related use for the material and the user has permission of [person], images or videos must not be downloaded,

Using the Firm’s internet or intranet access for accessing, downloading or receiving any offensive, obscene, lewd or indecent material is forbidden and will be considered as gross misconduct which may result in summary dismissal. For the avoidance of doubt such material, includes, but is not limited to, anything which is, in the opinion of the Partners, repulsive, indecent or offensive, such as any material of a sexual nature whether written or pictorial.

We use independently supplied software and data to identify inappropriate or sexually explicit internet sites or e-mails. The Firm may block access from within the network to any websites which it considers to be inappropriate for users to access.

Anyone who uses the Firm’s computer systems in an attempt to disable, defeat or circumvent any security facility designed to protect the Firm’s computer systems will be the subject of disciplinary action which may result in summary dismissal.

**This Policy and the Firm’s Disciplinary Procedure**

A breach of any of the provisions of this policy will be treated in accordance with the Firm’s Disciplinary Procedure. In certain circumstances, a breach may amount to gross misconduct leading to summary dismissal.

**Monitoring**

Under the Regulation of Investigatory Powers Act 2000 and the Lawful Business Practice Regulations 2000, the Firm is entitled to monitor e-mails and the use of the internet at work to check that they are business-related. These systems belong to the Firm and are connected to the outside telecommunications system.

The Firm monitors e-mail traffic (including content) and use of the internet (including sites visited) in order to ensure that all such systems are being used for legitimate business purposes and in order to monitor quality of service and effectiveness of training.

If business needs dictate, the Firm also checks voice mail boxes and business e-mails in users' absence and may also access and review any user's computer system, including any files or e-mails stored, if this is necessary for another user's work or for business needs generally. This will only be carried out with the prior authority of the [Senior Partner].

The Firm also reserves the right to carry out such monitoring and recording where it has reasonable grounds to believe that criminal offences or breach of the Firm’s rules and procedures may be taking place.

This notice informs all users that the Firm carries out such activities. If users do not want private material viewed, read or monitored, they should ensure that no such material is kept on the Firm’s computers or telephone systems.

**Compliance**

Any incidents which may breach this policy will be dealt with promptly. A manager can request that a user’s computer (including its storage devices) be investigated for evidence of a suspected breach of this policy.

**Social Media**

The Firm recognises the increased use of social media by staff, in particular in the course of their private communication eg Facebook, MySpace and similar forums. While the Firm recognises the right of all staff to access these media, they should never be used in such a way as to harm the Firm or the user’s relationship with colleagues, neither should they be accessed at work, other than in breaks or at lunchtime, as this is likely to impede work performance. In particular, users must not use social media so as to

1. breach this Policy
2. breach the Firm’s obligations to any regulatory bodies
3. breach any professional obligation of confidentiality
4. defame or disparage the Firm , clients, business partners, suppliers or other stakeholders
5. harass or bully their colleagues in any way
6. unlawfully discriminate against colleagues or third parties
7. waste time at work
8. breach any other law or ethical standards

If users are found to be in breach of this policy, they are likely to be subject to disciplinary action which may lead to their dismissal

I confirm that I have read and understood the contents of this Computer Use Policy and agree to abide by the terms stated therein. I consent to the Firm monitoring and intercepting incoming/outgoing e-mail, voicemail and Internet use for legitimate business reasons and to ensure that this policy is being adhered to. I agree that the Firm may inspect its computer equipment supplied to me or in my possession or control in the event it is suspected by management that I have breached the terms of this policy.

Signed:...........................................Date:..........................................

Please print name.

1. State here the name of the Firm or Company, the term ‘Firm’ is used throughout the document, but in the case of Companies, users will need to substitute ‘Company’ as applicable and where the term ‘Partner’ is used, substitute ‘Director ’as necessary [↑](#footnote-ref-1)
2. State here the name of the person who has responsibility for IT within the business, subsequently shown as [person] in this Policy [↑](#footnote-ref-2)