ELECTRONIC COMMUNICATIONS AND INTERNET POLICY –

GUIDANCE NOTE AND TEMPLATE POLICY

When employing staff it is useful to create a policy which sets out your standards and requirements of your staff when they are using electronic communications or the Internet.

From this guidance note you will understand the reasons for having such a policy and the law surrounding this area. The template policy will provide you with an outline of a policy but you must consider the appropriateness of this for your social enterprise and seek legal advice if you are unsure.

For further information please also see
http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles;
http://ico.org.uk/for_organisations/data_protection/topic_guides/employment

DLA Piper has produced these helpsheets as part of a collaborative project with UnLtd. DLA Piper is one of the largest business law firms in the world with an extensive pro bono legal advice programme which assists social enterprises, charities and individuals across the globe. UnLtd is the leading provider of support to social entrepreneurs in the UK and offers the largest such network in the world.

ELECTRONIC COMMUNICATIONS AND INTERNET POLICY – GUIDANCE NOTE (TO BE USED BY EMPLOYERS)

When employing staff it is useful to create a staff handbook containing key policies and procedures. This guidance relates to creating a policy for employees' usage of standard electronic communications and the Internet and it should be read alongside the electronic communications and Internet policy precedent ("**Policy**").

The Policy may be used as part of a company handbook or as a free-standing policy on the acceptable use of electronic communications, the web and other IT at work.

Over and above time wasting and loss of productivity, improper or unauthorised use of such resources can carry significant legal and business risks for an employer. The legal risks may include: breaching intellectual property law by using images, articles, etc. without the owner's permission; and claims of harassment, constructive dismissal, discrimination or defamation by other employees (i.e. publishing something untrue about another person or company, which damages their reputation). The business risks may include damage to the employer's reputation. The Policy is intended to help an employer reduce such risks and should be drafted to take into account the type of business it is to apply to and the IT systems that the employer has in place.

1. INTRODUCTION

Employment policies should generally say that they are not binding contracts (i.e. they should be 'non-contractual'), to allow the employer flexibility to change them as necessary without having to seek the agreement of the workforce. Further, ensuring that a policy is non-contractual reduces the employer's risk that a failure to adhere to such policy amounts to a breach of an employee's contract of employment.

Even if a policy is said to be non-contractual, if it gives important instructions to employees about the performance of their jobs or their conduct, employees may still be under an express or implied obligation to comply (for example, see clause 12.4 of the precedent contract of employment which expressly obliges an employee to comply with the company's data protection policy).

2. TYPES OF MONITORING

Methods by which employers may seek to monitor employees' use of electronic systems include (amongst others):

- using programs designed to search the content of e-mails sent by an employee by "key-word" or destination addresses;
- monitoring and blocking particular Internet sites; and
- monitoring and recording telephone conversations to assess performance and quality or to ensure that no illegal activities are carried out.

Monitoring can be in the form of spot checks, specific checks or monitoring conducted on a random basis. In any event, an employer should make sure they do not unfairly target employees during monitoring as to do so could open up a claim for discrimination.

3. LEGISLATION

There are various pieces of legislation which relate to employees' use of electronic communications and the employer's right to intercept and control this.

3.1 Data Protection Act 1998 ("DPA") and Employment Practices Data Protection Code ("Code")

If use by employees of electronic communication systems and monitoring is likely to involve the processing of personal data, it will be regulated by the DPA, together with the Code. The aim of the Code is to help employers comply with the DPA and to encourage them to adopt good practice. Employers should familiarise themselves with the eight data protection principles under Schedule 1 of the DPA, and Part 3 of the Code which contains guidance on monitoring at work including good practice and recommendations.

In summary, the eight data protection principles under the DPA are that personal data must be:

- processed fairly and legally;
- gathered only for specified and legal purposes;
- appropriate to the purposes for which it is collected;
- accurate and, where necessary, kept up to date;
- kept only for as long as required;
- regulated in its processing and protected in its storage by putting in place appropriate measures; and
- kept within the European Economic Area, unless the external country or territory ensures adequate protection for the rights and freedoms of those who are the subject of the personal data being processed.

These principles are set out in full, together with useful and comprehensive guide, on the website of the Information Commissioner's Office at the following address: http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles.

The Code can also be accessed in its entirety along with its own guide on the Information Commissioner's Office's website at the following address: http://ico.org.uk/for_organisations/data_protection/topic_guides/employment

Employers should have good reason to depart from the Code and its action points, or risk breaching the DPA.

3.2 Regulation of Investigatory Powers Act 2000 ("RIPA")

RIPA regulates certain types of monitoring, including the interception of a communication in the course of transmission (by means of a public postal service, or a public or private telecommunication system – this would include emails).

To intercept a communication in the course of its transmission means to:

- modify or interfere with the telecommunication system or its operation;
- monitor transmissions made via the system; or
- monitor transmissions made wirelessly to or from apparatus making up part of the system in order to make the contents of the communication available, while being transmitted, to a person other than the sender or the intended recipient.

It is important to note that this includes storing the intercepted content of the communications to be monitored later, even if it is not read immediately. This activity is made illegal by RIPA, with limited exceptions including obtaining a warrant from the Secretary of State. Those exceptions that may be relevant to employers are:

- where the interception takes place with the consent of the sender and receiver, or when the employer reasonably believes that both have consented; and
- where the interception is connected with the operation of the communications service itself.

3.3 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("Telecommunications Regulations")

The Telecommunications Regulations provide for circumstances where employers are allowed to intercept business communications without consent from the sender and intended recipient. These circumstances are:

- Monitoring or keeping a record of communications:
  - To establish the existence of facts;
  - To ascertain compliance with regulatory or self-regulatory practices or procedures;
  - To ascertain or demonstrate the standards which are achieved or ought to be achieved by people using the system in the course of their job;
  - In the interests of national security;
  - To prevent or detect crime;
  - To investigate or detect unauthorised use of the system;
  - To ensure effective operation of the system;

- Monitoring (but not keeping a record of) communications to determine whether they are relevant to the business; or
- Monitoring (but not keeping a record of) communications made to a confidential telephone counselling or support service that is free of charge and allows users to remain anonymous if they wish.

A selected list of some of these circumstances is also set out in paragraph 2.2.1 of the Policy, which lets the employees know that there are situations in which the company can and may monitor their emails. The employer should include those that will be relevant to their business in this list.

3.4 Human Rights Act 1998

It is clear from European case law that if monitoring is to take place, employers should have an electronic communications and Internet policy in place and employees should be informed that they might be subject to monitoring. Employees should understand when information as a result of monitoring is likely to be obtained, why it is being obtained, how it will be used and the identity of anyone who the information will be disclosed to. Paragraphs 2.2, 3.1.2 and 3.1.4 of the Policy address this issue, however, any further ways in which electronic communications or Internet use is monitored should also be detailed in the Policy.

3.5 Other

There is implied into employment contracts a mutual duty not to act in a manner that could destroy or seriously damage the relationship of trust and confidence between the employer and employee (i.e. the implied term of mutual trust and confidence). In addition to becoming familiar with those statutes and regulations listed at paragraph 2.2.1 of the Policy, an employer should ensure that its monitoring activities do not constitute a breach of its duty of trust and confidence. If this duty is breached, an employee may bring a claim for constructive unfair dismissal.

4. E-MAIL USE

Employers should appreciate that the informality and immediacy of e-mail communication can create additional risks when compared to more traditional written communications. For example, e-mails can be easily misdirected, very quickly disseminated and are very hard to destroy.

Whilst some employers tolerate occasional personal use of e-mails, others do not and therefore, paragraph 2.1 of the Policy should be amended accordingly. It is possible for an employer to only permit personal use of e-mails during break times or outside working hours. In the event that occasional personal use of e-mail is permitted, employees should be encouraged to mark any personal e-mails as such in the subject header. The Policy assumes that limited personal use of the e-mail system is permitted.

Employers may consider blocking access to web-based personal email accounts (e.g. Hotmail and Yahoo) because of their potential to overload a system or introduce viruses. If they choose to block them, the Policy should specifically address this.

Depending on the type of business, employers are likely to differ greatly in their approach to record keeping. If employees will not be required to keep file copies of business e-mails for record keeping purposes, paragraph 2.4 of the Policy should be amended accordingly.

5. INTERNET USE

Like personal use of e-mail, some employers tolerate occasional personal use of the Internet, whilst others do not. Paragraph 3 of the Policy should be amended according to the employer's preference. The Policy assumes that limited personal use of the Internet is permitted during lunch hours and outside working hours.

An employer may consider blocking sites facilitating online radio, audio and/or video streaming because of their potential to introduce viruses or overload a system. If so, the Policy should specify this.

6. SYSTEMS AND DATA SECURITY

The wording in the Policy is intended to be applicable to a broad range of organisations. An employer should tailor this section in light of its own particular IT infrastructure and security needs or seek legal advice.

7. PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF POLICY

Whilst an employer may decide that the company's Board of Directors should have overall responsibility for the policy, it is usual for the implementation of the policy to be delegated to a more appropriate officer, which would usually be a senior member of the IT team (see paragraph 5.1 of the Policy).

ELECTRONIC COMMUNICATIONS AND INTERNET POLICY

1. INTRODUCTION

1.1 The Company has made a significant investment in information technology and electronic communication systems which enable our employees to work efficiently. Electronic messaging or e-mail has become a vital tool of communication alongside methods such as fax, telephone and post. Whilst e-mail can contribute to improving communication between colleagues and external contacts, it is essential that it is used properly to maximise its benefits and avoid problems. Likewise, access to the Internet can increase effectiveness and productivity but also poses potential security risks.

1.2 This policy covers all individuals working for the Company at all levels and grades including senior managers, officers, directors, employees, contractors, trainees, homeworkers, part-time and fixed-time employees and agency staff (collectively referred to in this policy as "employees") [and also third parties who have access to the Company's electronic communications systems].

1.3 The purpose of this policy is to set out standard working practices as to the use of electronic communications systems provided by the Company. This policy is for guidance only and does not form part of the contract of employment. Breach of this policy may be dealt with under the disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

1.4 This policy should be read in conjunction with the Company's policies on social media, data protection, discipline, grievance and bullying and harassment.

1.5 The sections below deal mainly with the use (and misuse) of computer equipment, e-mail, Internet connection, telephones, Blackberries, personal digital assistants (PDAs) and voicemail but this policy applies equally (where relevant) to the use of fax machines, copiers, scanners, CCTV and electronic key fobs and cards. The Company's employees are expected to have regard to this policy at all times to protect its electronic communications systems from unauthorised access and harm.

1.6 The Company's e-mail and Internet systems and any documentation or correspondence produced using these systems is the property of the Company. It is vital that employees read this policy carefully. If there is anything an employee does not understand, it is their responsibility to ask their manager to explain.

2. E-MAIL USE

Employees should ensure they are aware of and comply with rules 2.1 to 2.9 which govern the use of e-mail within the Company.

2.1 The Company's e-mail system is primarily for business use

Occasional and reasonable personal use is however permitted provided that this does not interfere with the performance of your duties or the operation of the Company's business or the system. you must not originate or distribute chain letters or other "junk" or "spam" e-mail. Avoid sending trivial messages, jokes or gossip by e-mail. You should not have any expectation of privacy in respect of personal use of the e-mail although the Company will only open

clearly personal e-mail communications where it is necessary for business purposes. In general you should not send or forward any private e-mails at work which you would not want a third party to read. Guidelines on the monitoring of e-mail are set out below.

2.2 All e-mail is stored and e-mail (including personal e-mail) sent and received by an employee may be inspected, examined or monitored by the Company without notice

2.2.1 The Company reserves the absolute right to review, audit and disclose all matters sent over the system or placed in its storage to the extent permitted by relevant legislation including the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The Company may carry out monitoring of e-mails for the following purposes:

2.2.1.1 in order to establish the existence of facts relevant to the business, eg to obtain records of transactions;

2.2.1.2 in the interests of national security;

2.2.1.3 to detect/prevent crime, eg to conduct investigations into suspected fraudulent transactions/corruption;

2.2.1.4 to detect the unauthorised use of a telecommunications system (eg to monitor use of the system to ensure that employees are not in breach of any policies or procedures relating to use or behaviour);

2.2.1.5 to ensure employees are achieving the standards required and to demonstrate the standards that ought to be achieved – this will include monitoring for quality control and staff training purposes;

2.2.1.6 to ensure the effective operation of the system, eg to protect a business network against computer viruses or from being accessed by hackers;

2.2.1.7 to determine whether the purpose of an e-mail is relevant to the business, eg checking an employee's e-mail during absence;

2.2.1.8 to ascertain the Company's compliance with regulatory and self-regulatory practices or procedures.

2.2.2 Wherever possible monitoring will be limited to traffic and subject records. However, the Company may monitor the content of the e-mails where this is necessary to the business. For example, where monitoring of traffic data reveals a suspected disciplinary offence, the Company may monitor the contents of the e-mail in order to conduct a fair investigation. In addition, the content of e-mails may be monitored for quality control reasons or to respond to business e-mails during employees' absences. Monitoring may take place at any time, both inside and outside office hours, but is most likely to be in the form of audits and/or spot checks. If monitoring reveals unauthorised use or any serious or repeated breach of this policy or any other form of use potentially damaging to the business, this may lead to disciplinary action including dismissal.

2.2.3 Employees should be aware that deleting a file or e-mail may not eliminate a message from the system and therefore may still be accessed by the Company. However the Company will not usually monitor e-mails that an employee has deleted from their personal computer without delay.

2.2.4 Whilst limited personal use of the e-mail system is permitted, employees have no expectation of privacy in respect of personal or business use. The Company may monitor personal e-mails in particular to detect excessive or otherwise inappropriate use.

2.2.5 An employee who receives an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material it should not be used or disclosed in any way.

2.3 Never send by e-mail illegal, discriminatory, defamatory, obscene, pornographic, harassing or otherwise abusive or threatening messages or material

2.3.1 In accordance with the Company's [equal opportunities/diversity] policy, the Company does not tolerate any

form of discrimination, and in particular, discrimination based on another's sex, race, disability, religion or belief, sexual orientation or age. Employees must not, therefore, send any e-mails which could be capable of being discriminatory. Employees should be aware that whether a remark is discriminatory will depend on how it is received, regardless of the intention of the sender. Such messages could result in liability not only for you but also the Company. If such messages are received they should not be forwarded and should be reported to the IT department.

2.3.2 If a recipient asks an employee to stop sending them personal messages then always stop immediately. If an employee feels that they have been harassed or bullied, or are offended by material sent to them by a colleague via e-mail, the employee should inform their line manager who will usually seek to resolve the matter informally. If this informal procedure is unsuccessful or employees do not want to raise this with their line manager, employees should refer to the grievance procedure.

2.3.3 Users of e-mail may be held to account for making defamatory remarks via e-mail. A defamatory statement is one which tends to damage the reputation of another individual or company. Employees must not participate in office gossip and/or spreading rumours over the e-mail system, which may seem innocent but can give rise to liability for defamation.

2.3.4 Sending abusive or threatening e-mails or obscene or pornographic attachments via the e-mail system are gross misconduct offences which are liable to summary dismissal. In addition, they may attract criminal liability.

2.3.5 All of the above may result in disciplinary action being taken including dismissal.

2.4 Always make hard copies of e-mails for record keeping purposes

Ensure that you keep file copies of all business e-mails, as you would for postal or faxed correspondence. Ensure that you obtain confirmation of receipt of important messages. If you do not obtain a delivery receipt, phone to check the recipient has received the e-mail. Failure to follow this rule may be treated as a disciplinary matter.]

2.5 Beware of viruses

Always scan before opening or sending attachments or immediately on receipt of any software or data source received from an external source. If employees are unsure of how to scan an e-mail please contact _____. Failure to scan for viruses is a disciplinary offence.]

2.6 Do not distribute documents, pictures, music or works of others without the owner's permission as this may infringe copyright laws

2.6.1 In particular, if employees are permitted to download articles and other materials from the Internet, they need permission from the author before using such information for business purposes.

2.6.2 The dissemination of copyrighted information is a disciplinary offence which may result in disciplinary action being taken against you including, in serious cases, dismissal. If in doubt, employees should speak to their manager about whether a particular work is copyrighted.

2.7 Never send confidential information by e-mail without express permission from the customer/external contact

2.7.1 E-mails are neither confidential nor secure. They are readily accessed by people other than the intended recipient. Employees should agree with the recipient that communication will be made by e-mail before sending or receiving e-mail. Failure to do so is a disciplinary offence which may result in disciplinary action being taken, including dismissal in serious cases.

2.7.2 The Company may take disciplinary and/or legal action for disclosure of confidential information regarding or belonging to the Company by e-mail during or after termination of employment. Contracts of employment outline the types of confidential information that employees are prohibited from disclosing during and on termination of employment.

2.8 Do not enter into contractual commitments by e-mail without authority and legal advice

2.8.1 E-mail is capable of forming or varying a contract in just the same way as a written communication. Because of the perceived informality of e-mail, there is the danger of contracts being inadvertently formed by employees, to which the Company is then bound. Employees must comply with the following rules before entering into contracts by e-mail.

2..8.2 Employees must obtain authorisation before negotiating contracts by e-mail. Take advice from a manager before entering into contractual commitments. [Managers should always seek legal advice.]

2.8.3 Employees must include the statement "subject to contract" in all e-mails if conducting contractual negotiations via e-mail until such time as it is intended that a binding contract should come into existence.

2.8.4 Employees must be satisfied of the legal identity of the other contracting party before entering into a binding contract via e-mail.

2.8.5 Failure to follow these rules is a serious disciplinary offence which may result in disciplinary action, including dismissal.

2.9 Remember that a damaging or confidential e-mail may have to be disclosed in litigation or in investigations by other authorities

E-mails should be regarded as a substitute for written communication and not conversation. Ill considered messages could have serious repercussions for the sender and the Company. E-mails may be stored on the system's hard drive after they have been deleted and these records are likely to be disclosable in legal proceedings in addition to e-mails which have been saved or retained in paper form.

2.10 In addition to the above rules, the following guidelines should be followed when using the e-mail system

2.10.1 Always maintain a professional image. Ensure the style and content of the e-mails is appropriate.

2.10.2 Employees should always consider if e-mail is the appropriate medium for a communication. Do not use e-mail for urgent messages; use the telephone. It should be noted that the delivery and integrity of e-mail cannot be guaranteed.

2.10.3 Respond to e-mails in a timely and professional manner. Always acknowledge receipt of e-mails requiring responses even if you cannot reply fully straight away.

2.10.4 Always consider the tone and content of e-mails. Remember also that email which contains personal data about an individual may be disclosed to that individual as a result of a data subject access request. Refer to the Company's data protection policy for more information.

2.10.5 When corresponding with customers or other external business contacts via e-mail, ensure that you insert the corporate disclaimer message.

2.10.6 Send e-mails to only those recipients/ groups for whom the e-mail is intended.

2.10.7 Only use plain text in e-mails. Fonts, underline, colour, graphics and tables may be lost in external e-mails and may adversely affect delivery times.

2.10.8 Ensure the subject matter is clearly indicated in the heading of e-mails.

2.10.9 Re-read and spell check messages prior to sending to ensure accuracy and clarity.

2.10.10 Identify the sender and other contact details in e-mails.

2.10.11 When sending attachments with external e-mails agree with the recipient the format to be used, e.g. Word 7, Excel, etc.

2.10.12 [Avoid using graphics if at all possible as these are very large files and can easily clog up the e-mail systems.]

2.10.13 Read and delete e-mails regularly. Workers should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling and use an out of office response when out of the office for more than a day.

2.10.14 Keep all passwords secure and do not disclose to unauthorised persons.

2.11 Employees are expected to follow these guidelines as a matter of good practice. If you do not comply with these guidelines, you may be subject to disciplinary action under the Company's disciplinary procedures.

3. INTERNET USE

The Company's computer systems are for business use. The Company encourages authorised employees to access the Internet during working hours, when direct work related benefits can result. However, limited personal use of the Internet is permitted during lunch hours and outside working hours, subject to compliance with the Company's policies on the type of information that may be accessed.

3.1 General Rules on Internet Use

3.1.1 Different access for different types of personnel may be given. The Company reserves the absolute right to block access to certain Internet sites as it deems necessary.

3.1.2 The Company has software and systems in place that can monitor and record all Internet usage. Employees should be aware that our security systems are capable of recording (for each and every user) each website visit, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time as is necessary for business purposes.

3.1.3 Whilst employees are permitted to reasonable use of the Internet during lunch hours and outside working hours, no employee should have any expectation of privacy as to his or her Internet usage.

3.1.4 We reserve the right to inspect any and all files stored on the Company's computer resources in order to assure compliance with policy. We also reserve the right to monitor the types of sites being accessed and the extent and frequency of use of the Internet at any time, both inside and outside office hours to ensure that the system is not being abused and to protect the business from potential damage or disrepute.

3.1.5 The display of any kind of sexually explicit image or document on any system of the Company is a violation of the Company's policy and a gross misconduct offence which will be dealt with through the disciplinary procedure. Employees who access such material may be committing a criminal offence. Sexually explicit material includes:

3.1.5.1 any digital photograph or cartoon depicting male or female nudity or partial nudity (eg topless images);

3.1.5.2 any sexually explicit text including stories, jokes, reports, gossip;

3.1.5.3 any other material with sexual content which could be construed as offensive.

3.1.6 Sexually explicit material may not be archived, stored, distributed, edited or recorded using any Company network or computing resources.

3.1.7 [The Company uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of. If an employee connects accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program and report the site address to _____].

3.1.8 _____ internet sites that are cost related or have cost _____ implication terms of access must not be subscribed to without the prior authority of _____.

3.1.9 Any file that is downloaded must be scanned for viruses before it is run or accessed. Instructions on how to proceed are available from _____.

3.1.10 Any software or files downloaded via the Internet into the Company network become the property of the Company. Any such files or software may be used only in ways that are consistent with their licences or copyrights. Remember also that text, music and other content on the Internet are copyright works. Workers should not download or e-mail such content to others unless certain that the owner of such works allows this.

3.1.11 [Please refer to the Company's social media policy for details of the Company's specific rules governing social media sites.]

3.2 Gross Misconduct Offences

3.2.1 The Company's connection to the Internet may not be used for any of the following activities:

3.2.1.1 knowingly to violate any laws and regulations;

3.2.1.2 knowingly to download or distribute pirated software or data;

3.2.1.3 deliberately to introduce and/or pass on any virus, worm, Trojan horse, or trap door program code;

3.2.1.4 disabling or overloading any computer system or network, or circumventing any system intended to protect the privacy or security of another user;

3.2.1.5 excessively accessing the Internet for personal use during business hours;

3.2.1.6 posting anything which could be construed as discriminatory, offensive, derogatory or defamatory about any of the Company's employees on any Internet site;

3.2.1.7 downloading entertainment software or games, or playing games against opponents over the Internet or Intranet;

3.2.1.8 uploading or distributing any software licensed to the Company or data owned or licensed by the Company; or

3.2.1.9 knowingly downloading pornographic or sexually explicit or otherwise offensive material.

3.2.2 Violation of any of the above whether in or outside working hours will be regarded as a gross misconduct offence which is liable to disciplinary action including dismissal.

3.2.3 Violation of some of the above may also constitute a criminal offence.

3.2.4 Use of the Company's Internet access facilities to commit breaches such as misuse of the Company's assets or resources, harassment, unauthorised public speaking and misappropriation or theft of intellectual property are also prohibited by general Company policy and will be dealt with under the relevant provisions of the Company Handbook.

3.2.5 The Company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries and archives on individuals' Internet activities.

3.3 Equipment security and passwords

3.3.1 Employees are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy. If given access to the e-mail system or to the Internet, employees are responsible for the security of their terminals and, if leaving a terminal unattended or on leaving the office, should ensure that they log off to prevent unauthorised users accessing the system in their absence. Employees without authorisation should only be allowed to use terminals under supervision.

3.3.2 Desktop PCs and cabling for telephone or computer equipment should not be moved or tampered with without first consulting the IT department.

3.3.3 User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. Company policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites. However, where access is to common sites that are approved subscription sites accounts IDs will be provided.

3.3.4 The Company has installed security systems to ensure the safety and security of the Company's networks. Any employee who attempts to disable, defeat or circumvent any firm security facility will be subject to disciplinary procedures which may lead to dismissal.

3.3.5 Employees who have been issued with a laptop, PDA or Blackberry or USB memory stick must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access

to data kept on such equipment to ensure that confidential data is protected in the event that the equipment is lost or stolen. Employees should also observe basic safety rules when using such equipment, such as not using or displaying it obviously in isolated or dangerous areas. Employees should be aware that if using equipment in a public place, documents may be read by other people.

4. SYSTEMS AND DATA SECURITY

4.1 Employees should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming the Company's business or exposing it to risk. Employees should not download or install software from external sources without authorisation from the IT department. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Files and data should always be virus checked by IT before they are downloaded.

4.2 No device or equipment should be attached to our systems without the prior approval of the IT department. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

4.3 Employees should not attempt to gain access to restricted areas of the network or to any password protected information unless specifically authorised.

4.4 Employees using laptops or wi fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the IT department from time to time against importing viruses or compromising the security of the system.

5. PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF POLICY

5.1 The Company's Board of Directors has overall responsibility for this policy but has delegated day to day responsibility for overseeing and implementing it to _____. The IT department will deal with requests for permission or assistance under any provisions of this policy, subject to their primary and priority tasks of maintaining our core systems, and may specify certain standards of equipment or procedures to ensure security and compatibility.

5.2 Managers have a specific responsibility to operate within the boundaries of this policy, to facilitate its operation by ensuring that employees understand the standards of behaviour expected of them and to identify and act upon behaviour falling below these standards.

5.3 All employees are responsible for the successful operation of this policy and should take time to ensure they read and understand it and to disclose any misuse of the Company's electronic communications systems of which they become aware to_____. Questions regarding the content or application of this policy should also be directed to _____.

Name of Employee:

Position:

I hereby confirm that I have received and read a copy of the Company's Electronic Communications and Internet Policy.

Signed _____

[Name of employee]

Dated_____

If you have finished with this document, please pass it on to other interested parties or recycle it, thank you.

www.dlapiper.com