ELECTRONIC COMMUNICATIONS POLICY

This policy sets out rules relating to the use of the Company's computer, telephone and facsimile, including Company laptops and mobile telephones. It applies to all users of the Company's telecommunications systems whatever their employment status and whether used at or away from the workplace. Any breach of this policy will be taken seriously and may lead to disciplinary action, which could include summary dismissal, under the Company's disciplinary procedure.

If you are unclear about the effect or meaning of any part of this policy, you should seek clarification from your departmental manager before you use the computer or telephone system. This policy may be changed from time to time.

1) PURPOSE OF THIS POLICY

The purposes of this policy is:

- To ensure that the computer and telephone resources are used properly.
- To establish clear rules on the extent to which you may use e-mail, internet and telephone facilities, both in the office and remotely, for personal use.
- To inform you that extended monitoring is taking place and the reasons for it.

2) COMPUTER USE

INTRODUCTION

The use of the internet, e-mail (both internal and external) and the computer system carries serious risks for the Company. E-mail, although often seen as an informal method of communication, should be seen as equivalent to writing a letter on Company paper.

Careless use of the Company's e-mail and internet system can have serious consequences. For example, it is possible to create a legally binding contract by exchange of an e-mail and confidential information may be deliberately or accidentally sent to the wrong people.

In addition, misuse of the internet and e-mails can introduce viruses into the network, infringe copyright laws and result in the harassment or defamation of others. For these reasons, the Company imposes strict limits on the internet and e-mail use in relation to both business and personal use.

VIRUSES

The introduction of viruses into the Company's computer system is potentially devastating. Although the Company has installed anti-virus software, this does not guard against all viruses. You should be aware that viruses can be introduced via e-mail attachments, CD-ROMs, floppy disks, portable storage media and the internet.

It is your responsibility to take care when opening e-mail attachments, especially when they are not expected or they are from unknown sources. If in any doubt, please contact the departmental manager who will check whether it is safe to open the attachment.

You should never open attachments ending with '.exe, .com, .bat, .pif' without obtaining clearance from the departmental manager. You should not install any software that has not been approved or purchased by the Company. You should not download any material, including games and screensavers, from the internet, CD-ROMs or floppy discs, etc. without clearance from / the approval of your departmental manager.

SECURITY

You should not tell any unauthorised persons your password. You should not use another person's password or work station without authorisation. (You must logout and, where available, lock your terminal when not in use).

It is very easy to send an e-mail to the wrong person. You should be very careful to ensure that the e-mails you send are correctly addressed.

E-mail is not a secure way of sending information. E-mails can be intercepted by third parties and intended recipients can alter and/or forward e-mails without your knowledge. For these reasons you should not send, for example, personal information or information about employees and commercially sensitive information. If you are unsure about the content you speak to your departmental manager before sending.

E-MAIL CONTENT

When sending e-mails internally or externally you should exercise the same care as if you were sending a letter on Company paper.

You must not send, forward, distribute or retain e-mail messages that contain language that is abusive, aggressive or offensive. You must not make any improper or discriminatory reference to a person's race, colour, religion or belief system, sex, age, national origin, disabilities or physique when writing e-mails and must not forward or distribute any material which does so.

If you receive any such messages, you must immediately contact your departmental manager who will tell you what to do.

The effective operation of the network can be hindered when large attachments, such as video clips, music or pictures, junk mail, hoax virus warnings and e-chain letters are sent and received. You must not send and should ask others not to send such e-mails to you for non-business purposes.

It is possible to create legally binding contracts without intending to via e-mail correspondence. E-mail must not be used for communications that could lead to a binding contract being formed

or which would have the effect of obligating the Company in any way without prior authorisation/approval being given from your departmental manager.

COPYRIGHT

Most information and software that is accessible on the internet is subject to copyright or other intellectual property protection. Nothing should be copied or downloaded from the internet for use within the Company unless the material owner has given express permission, this includes screensavers, desktop pictures and music/sound files.

PERSONAL USE OF COMPANY COMPUTERS

The Company's computers, including laptops, are to be used solely for business purposes, subject to the following exceptions:

- You may make reasonable/limited use of the Company's computer system for sending personal e-mails outside your normal working hours or during your lunch break in accordance with the terms of this policy and having obtained the departmental manager's permission.

- You may use the internet for reasonable/limited personal use outside your normal working hours or during lunch break in accordance with the terms of this policy.

The Company reserves the right to withdraw permission for personal use in individual cases without giving reasons.

INAPPROPRIATE WEBSITES

You must not under any circumstances access inappropriate or offensive websites or distribute or obtain similar material through the internet or e-mail when using Company equipment, even if you are doing so in your own time. Examples of inappropriate or offensive material include racist material, pornography, sexually explicit images, text and related material, the promotion of illegal activity or intolerance of others and gambling sites or chat rooms.

The Company has the final decision as to whether it considers particular material to be inappropriate under this policy. If you are unsure whether particular material would be considered appropriate by the Company you should seek clarification from your departmental manager before accessing or distributing such material. If in doubt as to whether the Company would consider certain material inappropriate, do not access or distribute it.

If you receive material which contains or you suspect may contain inappropriate material or you access such material on the internet inadvertently, you must immediately report this to your departmental manager who will tell you what to do. You must not under any circumstances forward, show to anyone else or otherwise distribute the material.

3) HEALTH & SAFETY

The Company requires all members of staff to act in a manner that gives due regard to the Company's Health and Safety Policy with regards to these machines. Furthermore, all members of staff are required to act in such a way as to avoid damage or misuse of the equipment. Specifically, only authorised members of staff may remove any covers, lids, connections or components of the equipment unless instructed to do so by an authorised person.

4) COMPANY DATA & SOFTWARE

The following rules should be observed at all times:

a) Copying of software (executable program files and related licensed data files or Company documents) onto portable storage media (cassettes, tapes and disks – hard, floppy or optical [CD/DVD] or memory stick) or to a remote drive of the Company's Local Area Network, except for the purpose of security backup, is expressly forbidden unless carried out on the instruction of an authorised person.

b) No portable storage media may be taken out of the building except by an authorised person.

c) No portable storage media may be attached to or loaded into a computer unless it has been sanctioned by an authorised person and it has been checked for infection with illegal programs (viruses).

d) All staff must take care to avoid the deliberate or accidental damage, loss or theft of portable storage media and any erasure or corruption of the data contained therein.

e) The installation and use of any software (including, but not exhaustively, any executable program, screensaver or macro program) which has not been authorised by the Company onto any item of equipment provided is expressly forbidden unless approved by the Company. Staff are reminded that the provisions of the Computer Misuse Act 1990 allow for the criminal prosecution of persons found misusing computers.

f) The installation and use of any hardware which has not been authorised by the Company into any item of equipment provided is expressly forbidden.

g) All staff should be aware that the information held on computer at the Registry is of a sensitive and personal nature as covered by the Data Protection Acts 1986 and 1998 and that they therefore have a duty to preserve the integrity, accuracy and confidentiality of that information. Users should therefore ensure that access to that data is not available to persons not entitled to it. This includes having data visible on a screen or printout when a visitor is in the room.

h) Portable storage media (tapes, hard and floppy disks, CD's, DVD's, memory sticks, etc.) provided by the Company for use by staff remain the property of the Company at all times, as do the machine-readable contents of such media including personal PSM used to store Company information. This right of ownership is asserted under the terms of the Copyright, Designs and Patents Act 1988.

5) PERSONAL USE OF THE TELEPHONE

This policy applies to landlines and to Company mobile telephones.

You are permitted to make occasional/reasonable private telephone calls, whenever possible these should be made during your lunch/break times or outside of working hours. The following types of personal calls are never permitted:

- Calls to premium lines.
- Calls to chat lines.
- Overseas calls.

USE OF PERSONAL MOBILE PHONES DURING WORKING HOURS

The Company has established procedures for getting personal messages to employees in an emergency. The existence of these measures means that there should normally be no need for employees to use their personal mobile phones during work hours. Accordingly, the use of personal mobile phones is only permitted during official lunch or break times but prohibited during working hours.

Employees should ensure that their family and friends who may need to contact them in emergencies are aware of the Company number to call, that is 01543 374341.

MOBILE PHONES & DRIVING ON COMPANY BUSINESS

It is a criminal offence to use a hand held phone or similar device when driving (in this policy driving also includes time when you have stopped at traffic lights or during other hold-ups when a vehicle can be expected to move off after a short while). As a result you must:

- Not use a mobile phone whilst driving unless it is being operated by a hands-free unit.

- Only make or take calls whilst driving if a hands-free unit is fitted and operational at the time of the call and ensure that any such calls are kept as brief as possible. It is strongly recommended that even outgoing calls should not be made.

- Ensure that any mobile phones which are not hands-free are switched off whilst driving.

- Not answer the phone if it rings whilst you are driving when the hands-free unit is not in use; if this happens pull over when you can safely do so, switch off the engine and answer the call or retrieve the message. You must not stop on a hard shoulder to do this – you would be exposing yourself to a significant risk and a separate offence by doing so.

6) MONITORING COMMUNICATIONS

HOW DOES THE COMPANY MONITOR COMMUNICATIONS?

The Company logs and audits the use of Company telephones, including mobile telephones, fax machines, including e-mail and other computer use. In particular, all calls from extensions and from Company mobiles are logged and regularly audited. Auditing software has also been installed which will monitor e-mails being sent and received and any internet sites visited. The Company keeps back-up tapes that record all computer usage which are retained.

Where it has good cause, the Company may monitor and record the contents of telephone calls, facsimile, computer files and internet use and e-mails sent, received and stored. You should also be aware that your e-mails will be checked in your absence from work. Given this, you should not regard either business or personal communications on the Company's facilities as private.

PURPOSE OF MONITORING

The purpose of such logging, auditing, monitoring and recording are to:

- Ensure the effective operation of the Company's telecommunications systems and to maintain system security.
- Investigate and detect unauthorised use of the systems in breach of Company policies such as excessive personal use or distribution of inappropriate material.
- Check whether matters need to be dealt with in your absence.
- Investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or a third party.
- Pursue any other legitimate reason relating to the operation of the business.
- Monitor standards of work.

KMB JAN '07