MINTED BOX LIMITED - POLICY ON THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Version 2.0 28th November 2018 – Minor updates to reference the Information Security Policy

1. Provision of Company Information and Communication tools

The Company provides you with information and communications technology to carry out your job duties. This may include computers, landline phones, VoIP phones, mobile/smart phones, printers, fax machines, photocopiers and any other means of storing, copying and transmitting data. As such, these tools are principally intended to be used for business purposes.

Company-provided communication tools may also be used for *appropriate* personal activity during the working day, provided that such activity does not interfere with job performance, consume significant resources, give rise to additional costs or interfere with the activities of your colleagues. Excessive or inappropriate use of company communication tools may give rise to disciplinary action.

The Company does not permit or condone inappropriate use of its communication tools at any time, including any illegal activity such as "hacking" into private networks, downloading pornography from the Internet, breaches of copyright or data protection laws etc. As a guiding principle, any activity proscribed in this policy is inappropriate for personal use. Should such activity be discovered, the Company's disciplinary procedures will be invoked.

The Company permits personal use of communication tools on the express understanding that it reserves the right (for business purposes or as may be required by law) to review the use of, and to inspect all material created by or stored on, these communication tools (See also the section on "Privacy" below).

Use of Company-provided communication equipment constitutes acceptance of the Company's right to monitor communications and access files that are made on or with that equipment.

2. Company Property

Company-provided communication equipment, as well as all data, files and messages produced, transmitted or stored using such equipment, are and remain the property of the Company, and are subject to reasonable Company inspection on request.

Upon termination of your employment, you are responsible for returning all Company-provided communication tools that may be in your possession (laptop computers, mobile phones etc.), as well as all electronic data produced and stored on them, and for returning or destroying any duplicates or hard copies of such data.

You must look after Company-provided equipment as if it were your own property. If equipment is lost, stolen or damaged due to your negligence or abuse, the Company reserves the right to charge you an amount up to the cost price of replacement equipment. The amount of the charge, and a suitable method of repayment, will be determined at the time of the loss, based upon the circumstances.

If you fail to return any Company-provided equipment upon termination of employment, or if it is returned in a damaged condition, the Company reserves the right to make an appropriate deduction from your final payment.

3. Passwords

You are responsible for your personal password security and for actions taken when your passwords are used. You should not reveal your passwords to anybody other than to your manager upon request.

You should refer to Section 6 of the Information Security Policy regarding the requirements for password complexity and the use of Administrator level accounts.

You should not leave your computer logged on and unattended; lock the screen if you are going to be away from your desk for any length of time, particularly if you are working with confidential or personal data.

“Wallpaper” and screensavers, whether in the form of verbal messages or pictures, must portray an appropriate, professional image. The Company will require the removal of any inappropriate wallpaper or screensavers.

4. Software

It is the Company's express policy to pay for the software it uses. You must not load, use, store or transmit any unlicensed or unauthorised software or applications on any Company-provided computer or mobile/smart phone, whether situated on Company premises or off-site, under any circumstances.

If you believe that additional licences or software programs may be useful as a business tool, you should discuss this with your manager.

5. Virus Protection

Virus protection software is installed on all Company computers and you are responsible for ensuring it is regularly updated. You must never take any action that would circumvent virus protection. Please be especially careful of email attachments and executable programs imported from the Internet, which may contain viruses, Trojans, worms etc.

6. Use of Company-provided equipment by third parties

You must not permit friends, relatives or other third parties that are not employed by the Company to use your Company-provided equipment, nor must you knowingly permit colleagues to use your equipment for inappropriate purposes.

Non-Company personnel who may require access to Company-provided communication tools for legitimate purposes (e.g. clients or contractors) must first be provided with a copy of this Policy, and sign a written agreement confirming that they will comply with its provisions.

7. Privacy

The Company will not frivolously or maliciously invade your privacy. However, because Company-provided communication tools are principally intended for business purposes, your rights to privacy in this context are limited, and you should not expect information created, transmitted or stored on Company communication systems to remain private.

In addition to routine access for maintenance and upgrades, the Company is entitled to review your electronic messages, files and data without prior notice, in various circumstances, including (but not limited to) the following:

- Investigating alleged misconduct
- Investigating complaints that Company resources are being used to transmit discriminatory or offensive messages or otherwise infringe upon or violate any other person's rights
- Discovering the presence of illegal material or unlicensed software
- Counteracting theft or espionage
- Responding to legal proceedings that call for the disclosure of electronically stored evidence
- Investigating indications of impropriety.

8. Confidential information

In order to perform your job responsibilities, you are given access to confidential data that are vital to business operations. You must respect the confidentiality of such data.

Because of the highly public nature of the Internet and email, you must exercise particular care when accessing or transmitting business information via those channels.

You may not use portable storage tools such as memory sticks or external hard drives to copy or remove Company information for any reason without the express prior permission of your manager, who will grant such permission only for legitimate business reasons.

9. File Storage and Archiving

You are encouraged to create folders to keep your files and email records tidy, to ensure efficient working on your part, and to facilitate the retrieval of information by your manager if you are not at work. You should review the files you store on company computers for relevance on a regular basis, and transfer anything that is no longer current to an archive folder. Remember that files containing work-related or client-related information are the property of the Company and should be retained for future reference in the same way that paper files would be.

Please bear in mind that email and voicemail messages and electronically stored items are Company business records that may have legal and operational effect, just like traditional paper documents. Even though you may delete messages from your own computer, they may remain on recipients' computers or on the Internet indefinitely, therefore you should never exchange or upload any content which you may later regret.

10. The Internet

The Company provides Internet access for legitimate business use. Often, it is the most efficient means of finding out information or communicating with others. However, this is not always the case, particularly where lengthy download times may be involved, so consider whether there may be quicker and more effective ways to achieve your business objectives. You should not spend excessive amounts of time surfing the net, even for work-related reasons.

Be aware of copyright issues when downloading or copying data from the Internet. Just because it is easy to copy material electronically, that does not mean it is legal to do so. Most information available on the Internet is protected by copyright in the same way as physical materials like books and CDs are. Breaching copyright using Company equipment could result in the company having to pay substantial damages to the copyright owners, and in you being disciplined or dismissed. Familiarise yourself with the copyright conditions of the information you are looking at before you download or copy it.

Some websites are contain inappropriate or offensive images or data, and the Company reserves the right to log, monitor or block incoming and outgoing Internet traffic from those sites. If you inadvertently connect to sites that contain sexually explicit, racist, violent or other potentially offensive material, you must immediately disconnect and advise your manager that these sites are accessible, so that blocking action may be considered. The ability to connect to them does not imply that the Company condones the visiting of such sites.

You may use Company equipment to surf the net during the working day for *appropriate* personal purposes, e.g. checking your bank account, the sports results, the news etc. However, you are not under any circumstances to use Company equipment to access any inappropriate sites at any time; contravention of this rule will result in disciplinary action. If you order goods online, you may not arrange for them to be delivered to the Company's address without the express prior permission of your manager.

11. Email

Email is a tool provided by the Company to facilitate the conduct of work duties. Your work email accounts must only be used for messages and attachments relating to work. The Company reserves the right to inspect the contents of any emails sent or received by employees.

You may use your Company email account for *necessary and appropriate* personal messages, as long as this does not interfere with your work performance. Personal messages should be kept to a minimum.

You must never send out any email or attachment that might show the Company in an unprofessional light. Email must never be used to express racist, sexist, or otherwise offensive opinions, either inside or outside the Company. Inappropriate use of email will be investigated under the Company's disciplinary procedures.

Please be security conscious. Email is **not** private; messages can be intercepted or wrongly addressed, and are easily forwarded to third parties. Do not allow anyone else to use your email ID and password, or leave your email logged on and unattended so that others could interfere with it. You will be held responsible for any inappropriate email activity using your accounts. Similarly, you must not send out emails purporting to be somebody else, and you must not read other people's emails without their express permission. Please be careful when giving out your email address, so as to minimise the receipt of junk mail.

The Data Protection Act (1998), and the General Data Protection Regulations (2017) cover information stored on email as well as other media, so care must be taken if emails contain any "personal data", i.e. any information about a living identifiable individual, such as their name, home address, home phone number, personal email address etc. An obvious example would be the receipt, storage or transmission of candidates' CVs. Such data must not be collected without the person's knowledge, it must not be disclosed or amended except for the purpose for which it was collected, and it must be accurate and up to date. Particular care must be taken if the data is confidential or sensitive (e.g. contains information about medical conditions, political or religious beliefs etc.). The individual in question has the right to inspect what is held about him or her on the email system, to demand correction of inaccurate information, to request blocking or erasure of damaging information, and even to sue for damage caused by inaccurate information!

"Personal data" must not be kept for longer than is necessary, so emails should be stored in such a way that they can be easily identified, reviewed and archived when they are no longer needed. If hard copies are printed, they must be stored carefully and disposed of once they are no longer of use. (See also the section on "File Retention".) Transfer of "personal data" outside the European Economic Area is forbidden by the Act. If in doubt, you should seek guidance from your manager.

You must read and comply with the requirements set out in the Information Security Policy.

Finally, please remember that emails are Company property, just like any other electronic or paper files. On termination of your employment, you must turn over to your manager all email records in your possession. You must not delete any work-related emails at any time.

12. Social Media

Social media and networking sites such as Facebook, Twitter, LinkedIn etc. may be accessed on Company provided equipment during the working day for either personal or Company business purposes, provided that such activity does not interfere with your job performance or that of your colleagues. Excessive or inappropriate use of social media during working hours may give rise to disciplinary action.

If your job role involves posting tweets or updates on Company social media sites, then the followers and fans attracted to those sites are deemed to be followers and fans of the

Company, not yours personally. If you leave the Company's employment, you must not continue to use the same account or give the impression you are still a Company representative.

You are also reminded that any social networking activities you conduct on Company equipment must be lawful and appropriate and not in any way defamatory, malicious or likely to damage the reputation of the Company.

Furthermore, if you use social media at any time and in any context to make comments of a negative or inappropriate nature about the Company, its employees, clients, customers, suppliers or other business associates, which might damage the Company's reputation or interests, the Company reserves the right to investigate your actions through the disciplinary procedure.

13. Telephones and Voicemail

Telephones should be answered in a friendly but professional manner, and as promptly as possible. Company landlines may be used for reasonable personal use, but please bear in mind that company telephones are principally provided for business purposes, and excessive personal use may be grounds for disciplinary action.

When leaving voicemail messages, you should follow the same rules of professionalism that guide the use of e-mail.

14. Misrepresentation or Misuse of Technology

When using any Company-provided communication tool, you represent the Company. Email or Internet messages can be traced back to the Company as their source. Therefore, you must exercise caution to protect the reputation and interests of the Company.

Electronic forgery (misrepresenting your identity in any way while using electronic communication systems) is not allowed for any reason. You may not take any action to misrepresent the identity of the person responsible for a message. If you forward a message prepared by someone else, it should be sent "as is", or if changes are necessary, you must clearly indicate where the original message was edited e.g. by using brackets, asterisks, or other characters to flag edited text.

You must also recognise the other side of this issue, namely that others can misrepresent themselves. Therefore, you should be wary of electronic communication from unknown people.

Misuse of communication tools may interfere with business operations and may injure the Company or other employees. As a general rule, you should not create or send any message, using any technological medium, that you would not want an outside party to view. Ask yourself whether you would be happy to see this on the front page of the local newspaper, and if the answer is no, then the message is probably not appropriate!

Under no circumstances may any posting, voicemail or email originating from the Company violate the letter or spirit of any law, or any of the Company's policies.

Examples of unacceptable use of technology include (but this list is not exhaustive):

- Sexually explicit messages, images, cartoons or jokes
- Unwelcome propositions, requests for dates or love letters
- Profanity, obscenity, slander or libel
- Expressions of political beliefs
- Derogatory, defamatory, threatening, abusive, rude or offensive language

- Any message that could be construed as harassment or disparagement of others based on sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs
- Commercial or for-profit activities unrelated to Company operations
- Chain letters
- Excessive use of the technology for personal purposes
- Release of confidential, sensitive or proprietary information
- Any action that is illegal or harmful to the Company.

Misuse of Company-provided technological tools, or any other failure to comply with this policy will be investigated through the Company's disciplinary procedure.

DECLARATION

I declare that I have read, understood, and agree to be bound by, the provisions of the Company policy on Information and Communications Technology. I understand that any failure to comply with its provisions may lead to disciplinary action.

Signature: ……. Date: …….

Name: …… (please print)