markallengroup.com

USE OF THE E-MAIL/INTERNET SYSTEMS

1. **Introduction**

1.1 The Company's computer system contains an email facility, which is intended to promote effective communication within the organisation on matters relating to its business. The email system should therefore be used for that purpose. This means the email system should not be used for a purpose detrimental to your job responsibilities, for spreading gossip, or for personal gain or in breach of any of the Company's standard employment policies on issues such as sexual harassment.

1.2 Messages sent via email and the internet are to be written in accordance with the standards of any other form of written communication generated by the Company and the content and language used in the message must be consistent with good business practice. Messages should be concise and directed to those individuals with a need to know. General messages to a wide group should only be used where necessary.

1.3 The Company reserves the right to amend this policy from time to time.

2. **Legal actions**

Beware what you say in messages sent via email or the internet. Improper statements can give rise to personal or employer liability, and you are reminded that you should always work on the assumption that your message may be read by parties other than the addressee. Always remember that such messages, however confidential, or damaging, may have to be disclosed in court proceedings or investigations carried out by appropriate regulatory bodies.

3. **Prohibited uses**

3.1 The Company's email system should not be used to transmit, receive or store any messages or attachments which:

- defame any person; or
- harass any person, including without limitation, sexually harass, discriminate against any person based on that person's race, gender, disability, sexual orientation, age, ethnicity or religious beliefs; or
- breaches any copyright or other intellectual property rights without the proper consent of the owner of such rights; or
- contains obscene, pornographic, profane or sexually explicit material in any form; or
- you know contains a virus.

The above list of prohibited actions is by way of example only, and is not intended to be exhaustive.

You will be held responsible for any communication from your email account.

Your use of the internet must strictly conform to this email policy and with any Company internet usage policy, and must not hinder or interfere in any matter with your duties.

Any violation of this policy may result in disciplinary action, including in appropriate circumstances, dismissal.

3.2 Never send messages containing confidential information outside the Company whether to clients or otherwise unless you have the consent both of your manager and the intended recipient that it is in order to do so. Any employee breaching this provision may be subject to dismissal by reason of gross misconduct.

3.3 Employees must not use their work e-mail (eg. Microsoft Outlook or other desktop application) to distribute bulk e-mails. Any employee who wishes to send an e-mail to more than 50 addresses outside of the Company must use the Company's approved Email Management System (EMS) (eg. Adestra or other third party EMS system). Breach of this policy will be treated very seriously as it could lead to the Company breaching data privacy regulations, as well as the Company's domain being blocked. Seek the advice of the IT Director, if necessary.

4. Scanning

4.1 Never import files or unknown messages onto your system without having them scanned for viruses. Treat messages with attachments from unknown sources with suspicion. Seek the advice of the IT Director if you are in any way suspicious.

5. General rules

5.1 Should you receive a message, which has been wrongly delivered to your email address you should notify the sender of the message by returning the message to that person. If the message contains confidential information you must not disclose or use that confidential information. Should you receive an email which contravenes this policy, the email should be brought to the attention of your manager.

5.2 Make hard copies of emails/internet messages for your file when you need to in the same way you would any other correspondence.

5.3 Ensure that you obtain confirmation of receipt of important messages and print off the copies for your file if necessary.

5.4 Do not create email/internet congestion by sending trivial messages or unnecessarily copying messages, and regularly empty your directories of information you no longer need to retain. If not, your own machine will operate more slowly as will others on the network.

5.5 Do not advertise by email/internet or send messages for missing items unless genuinely urgent for business reasons. Unwanted junk mail annoys everyone.

5.6 Do not send any documents by email which include an individual's personal contact details unless that document has been password protected. Password should also be sent in a separate email or via another method. Under no circumstances should passwords be disclosed unless authorised by the disclosing party.

6. **Personal use of the internet/devices**

6.1 It is permissible to browse the world-wide web for incidental personal purposes, preferably outside normal working hours. This does not include a user incurring substantial expenditure of time or expense to the Company, uses for profit or uses that would otherwise violate Company policy with regard to employee time commitments or Company equipment.

The company reserves the right to terminate access to certain unsuitable sites including *Facebook*, and chat rooms.

6.2 Personal messages may be sent but these should respect the primary purpose of the email system. Employees must label personal email or messages as "personal", or must send personal messages only by means that clearly identify the message as being personal in nature. Any message sent without such labelling or identification, may be assumed to have been sent on behalf of the Company, to which the company will have access.

6.3 Employees are only permitted to use their own Bring Your Own personal devices (BYO Devices) within the Company workplaces via access to the Company's WiFI. Access to the Company's internal network is not permitted for BYO Devices.

6.4 All equipment that is connected to the internal network must be authorised and checked by a member of IT.

7. **Security**

7.1 You are responsible for the security of your terminal and you must not allow the terminal to be used by an unauthorised person. You should therefore keep your personal password confidential and change it regularly. When leaving your terminal unattended or on leaving the office you should log off/lock the system.

7.2 You are responsible for the condition, security and safety of any Company equipment when taken outside of the Company's workplaces. This includes laptops, mobile phones and the Company's pool IT equipment. You must receive authorisation from a member of the IT team and sign for receipt of all pool IT equipment before such item is taken.

7.3 Server access – All documents and files located on ANY server/desktop must be restricted to teams or individuals who require access. In particular, any folders which contains contact information must be restricted to specific individuals who understand and agree to the policy and controlled use of this information.

7.4 USB/removal devices that are used to transfer data/information owned by the Company should be encrypted. A member of the IT team must be instructed to carry out this task.

8. **Software**

8.1 The Company's computer software policy applies to all software (including fonts), which is loaded onto PCs and file servers belonging to the Company.

8.2 The Company licenses the use of computer software from a variety of outside companies. The Company does not own this software or its related documentation and, unless authorised by the software developer, does not have the right to reproduce it except for backup purposes.

8.3 In the case of Client/Server and network applications, you are expected to use the software only in accordance with the licence agreements.

8.4 You are not permitted to download or upload unauthorised software over the Internet and are expected to notify the Managing Director of any misuse of software or related documentation.

8.5 Under UK copyright law, anyone involved in the illegal reproduction of software can be subject to unlimited civil damages and criminal penalties including fines and imprisonment. The Company does not condone the illegal duplication of software. Anyone who makes, acquires, or uses unauthorised copies of computer software will be subject to disciplinary action under the Company's disciplinary procedures.

8.6 If you are in any doubt whether any particular software program can be copied you must ask the IT Director, and if necessary obtain his approval before proceeding.

9. Sabotage

9.1 Any deliberate or grossly negligent sabotaging of computer systems belonging to the Company or another organisation whilst utilising the Company's hardware, software or networks will constitute gross misconduct.

10. Data protection

10.1 The Company holds data about employees, customers and other individuals, which is subject to the provisions of the General Data Protection Regulations 2018 (GDPR). The responsibilities of all employees in regards to processing personal data are set out in the MAG Data Protection Policy, which all employees must read and agree to follow. If you wish to hold or process any data either internally or externally and have any concerns about your legal ability to do so, you should speak to the IT Director, Data Operators Director or Data Protection Officer.

10.2 Please refer to the Company's Data Protection Policy document for guidance on how to report or manage any data breach.

10.3 Data extractions including contact information can only be carried out by authorised personnel.

10.4 Contact information data can only be held and used by the company for a limited amount of time. Refer to the MAG's Data Protection Policy. Data/documents that fall outside of this policy must be deleted or marked as GDPR removed.

11. Systematic monitoring

11.1 The Company, as far as possible, respects its employees' desire for and expectation of privacy. The Company reserves the right, however, to engage in monitoring (including random monitoring) of website browsing, email messages or other electronic files created by employees. Such monitoring may include the monitoring of all material created, accessed and/or received

by an employee including but not limited to encrypted, password-protected and deleted material (including material recovered by the [IT Director which has been deleted from the relevant employee's system). It is in the interests of all employees to bear with these security actions, which are intended to establish innocence as well as guilt. Refusal to accede to reasonable requests of this nature may result in disciplinary action being taken. In signing and returning a copy of this policy, you consent to such monitoring.

12. **Acceptance of policy**

No employee may send emails using the Company system unless they have read this policy and confirmed in writing that they have agreed to the terms and conditions it contains.

To: Mark Allen Group of companies

I confirm that I have read and understand the above policy, and accept the terms and conditions it contains.

Name _____

Signed _____ Date _____