INFORMATION & COMMUNICATIONS SYSTEMS POLICY STATEMENT

This policy applies to all employees when they are using communication systems supplied by the Company, whether or not during working hours and whether or not from the Company's premises. Our IT and communications systems are intended to promote effective communication and working practices within our organisation, and this policy outlines the standards you must observe when using these systems.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

SCOPE OF THE POLICY

This policy deals with the use (and misuse) of computer equipment, email and internet, telephones, mobile telephones and voicemail. It also applies to the use of fax machines, copiers, scanners and any other communication or recording device.

SECURITY & PASSWORDS

Staff 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.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by your line manager. For the avoidance of doubt, on termination of employment staff must provide details of their passwords to their line manager and return any equipment belonging to the Company.

Staff are responsible for the security of their terminals and if leaving a terminal unattended or leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence.

Staff who have been issued with a laptop, mobile telephone or other communications equipment 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 confidential data is protected in the event of loss or theft. Any damage, loss or theft should be reported to the HR Director immediately. The Company reserves the right to make a deduction from your wages in respect of damaged or lost property, in

accordance with the Code of Conduct in the Employee Manual.

SYSTEMS & DATA SECURITY

Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

Staff are not permitted to download or install software from external sources without prior authorisation from the IT department. In addition, no device or equipment should be attached to our systems without the prior approval of the IT department. Illegitimately encrypting information is strictly prohibited.

We monitor all e-mails passing through our system for viruses. Staff should exercise caution when opening e-mails from unknown external sources, or where an e-mail appears suspicious. The IT department should be informed immediately if a suspected virus is received.

Staff should not attempt to gain access to restricted areas of the network, or to password-protect information, unless authorised to do so by management.

USE OF E-MAIL

Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform the HR Director.

It is the Company's policy not to store large numbers of e-mail messages. As a general rule, you should promptly delete each e-mail message that you receive after you have read it.

Staff should remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

In general staff should not:

a) Send or forward private e-mails at work which they would not want a third party to read

b) Send or forward chain mail, junk mail, cartoons, jokes or gossip
c) Sell or advertise using our communication systems or broadcast message about lost property, sponsorship or charitable appeals, without prior authorisation from management
d) Agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained, or
e) Send messages from another worker's computer or under an assumed name unless specifically authorised

Staff who receive a wrongly-delivered e-mail should return it to the sender.

USE OF THE INTERNET

Internet access is provided primarily for business purposes.

Staff should not access any web page or download any files from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral.

Staff should not under any circumstances use our systems to participate in any internet chat room or post messages on any internet message board.

USE OF SOCIAL MEDIA

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter and LinkedIn. However, employees' use of social media can pose risks to our confidential and proprietary information and reputation, and can jeopardise our compliance with legal obligations.

The following rules apply to the use of social media for both business and personal purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities or equipment belonging to members of staff.

Staff may be required to remove internet postings which are deemed to constitute a breach of Company policies. Specifically, employees are prohibited from using social media to:

a) Breach any obligations they may have relating to confidentiality
b) Breach our Disciplinary rules
c) Defame or disparage the organisation or its affiliates, employees, customers, clients, business partners, suppliers, vendors or other stakeholders
d) Harass or bully other staff in any way
e) Breach of our Equal Opportunities & Diversity policy

f) Breach our Privacy policy (for example, never disclose personal information about a colleague online)
g) Breach any other law or ethical standards

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author and the organisation.

If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager, who may impose certain requirements and restrictions with regard to your activities. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your manager.

If you see content on social media that disparages or reflects poorly on our organisation or our stakeholders, you should speak to the HR Director immediately. All staff are responsible for protecting our business reputation.

The contact details of business contacts made during the course of your employment are regarded as our confidential information, and as such you will be required to delete all such details from your personal social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

Upon termination of your employment with the Company, you should update your social media accounts immediately to reflect that you are no longer employed by us.

PERSONAL USE OF SYSTEMS

We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

The following conditions must be met for personal usage to continue:

a) Use must be minimal and take place outside of normal working hours (that is, during lunch hours, before your normal start time or after your normal finish time)
b) Use must not interfere with business or office commitments
c) Use must not commit us to any marginal costs, and
d) You must comply with our policies including the Equal Opportunities & Diversity policy, Anti-Bullying and Harassment policy, Privacy policy and the Disciplinary procedure.

Staff should be aware that personal use of our systems may be monitored and, where

breaches of this policy are found, action may be taken under the Disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.

MONITORING USE OF SYSTEMS

Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. The Company has the right, but not the duty, to monitor all communications and downloads that pass through its facilities, at its sole discretion. A CCTV system monitors the exterior and lobby of the building 24-hours a day and this data is recorded. Any information retained on the Company's facilities may be disclosed to outside parties or to law enforcement authorities in order to comply with our legal obligations in our role as an employer.

We reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is not exhaustive):

a) To monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy
b) To find lost messages or to retrieve messages lost due to computer failure
c) To assist in the investigation of wrongful acts, or
d) To comply with any legal obligation.

INAPPROPRIATE USE OF SYSTEMS

Misuse or excessive use or abuse of our communication systems or the internet in breach of this policy will be dealt with under our Disciplinary procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence.

In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

a) Pornographic material
b) Offensive, obscene or criminal material or material which is liable to cause embarrassment to us or to our clients
c) A false and defamatory statement about any person or organization
d) Material which is discriminatory, offensive, derogatory or may cause embarrassment to others
e) Confidential information about us or any of our staff or clients (which you do not have authority to access)
f) Any other statement which is likely to create any liability (whether criminal or

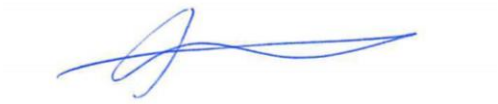
civil, and whether for you or us), or

g) Material in breach of copyright

Any such action will be treated very seriously and is likely to result in summary dismissal.

ACKNOWLEDGEMENT

By signing below, I acknowledge that I have read, understood and agree to comply with the foregoing Information & Communications Systems policy. I understand that if I do not comply with the policy, I may be subject to disciplinary action, including loss of access to the Company's facilities and discharge from employment. I may also be subject to legal action against me for damages or indemnification.

Signed 

Position CEO Date: 1 July 2023

In signing below I agree to adhere to the Company's Information & Communications Systems Policy.

Signed by employee:

Signed: …… Date: ……