HACKLE SECURITY SERVICES LTD

COMMUNICATIONS POLICY

This policy document regarding internet, email, telephone and media forms part of the terms and conditions of employment for employees of Hackle Security Services Ltd (the Company).

This policy applies to your employment at the Company and also at our clients' sites. This policy must be observed at all times, and employees must also comply with any policy or guidelines existing for our client sites.

EMAIL AND THE INTERNET

To maximise the benefits of our computer resources and minimise potential liability, employees are only permitted to use Hackle Security Services (the Company) computer systems, and those supplied by our clients for use in the course of your duties, in accordance with the Company's Data Protection and Monitoring Policies and the following guidelines.

GENERAL GUIDELINES

The Company's computer systems, software and their contents belong to the Company, and they are intended for business purposes. Employees are permitted to use the systems to assist in the performance of their duties.

The Company has the right to monitor and access all aspects of its systems, including data which is stored on the Company's computer systems in compliance with The General Data Protection Regulation (GDPR).

Employees must receive prior approval from management before using any part of the computer systems for personal use.

SECURITY

The Company requires employees to log on to the Company's computer systems using their own password *(where provided)* which must not be shared with other employees.

Employees are not permitted to use another employee's password to log on to the computer system, whether or not they have that employee's permission. If an employee logs on to the computer using another employee's password, he or she will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

Any employee who discloses his or her password to another employee will be liable to disciplinary action.

To safeguard the Company's computer systems from viruses, employees are not permitted to load or run unauthorised games or software, or to open documents or communications from unknown origins. Where the computer has Internet or electronic mail (e-mail) facilities installed, employees are not permitted to download or open files from the Internet. Whereby an employee receives communication from an unknown origin and has concerns that the content could/would corrupt the company systems the employee must forward incoming e-mail attachments to the designated IT specialist, for virus checking.

The Company reserves the right to require employees to hand over all Company data held in computer useable format.

USE OF EMAIL

The Company's computer systems contain an e-mail facility which is intended to promote effective communication within the Company on matters relating to its business. Employees should only use the e-mail system for that purpose. The Company encourages employees to make direct contact with individuals rather than communicating via e-mail.

E-mails should be written in accordance with the standards of any other form of written communication, and the content and language used in the message must be consistent with best Company practice, messages should be concise and directed to relevant individuals on a need to know basis.

E-mails can be the subject of legal action (for example, claims of defamation, breach of confidentiality or breach of contract) against both the employee who sent them or the Company. Employees are also reminded that e-mail messages may be disclosed to any person mentioned in them. Employees must therefore always be careful if they write an e-mail containing content that refers to a third-party.

MONITORING

Monitoring will not take place unless it is carried out in accordance with the Company's Monitoring Policy. Please refer to the Company's Monitoring Policy for further details.

INAPPROPRIATE USE

Misuse of the Company's computer systems may result in disciplinary action up to and including summary dismissal. Examples of misuse include, but are not limited to, the following:

- Sending, receiving, downloading, displaying or disseminating material that insults causes offence or harasses others.
- Accessing pornographic, racist or other inappropriate or unlawful materials.
- Engaging in on-line chat rooms or gambling.
- Forwarding electronic chain letters or similar material.
- Downloading or disseminating copyright materials.
- Transmitting confidential information about the Company or its clients.
- Downloading or playing computer games.
- Copying or downloading software.

SOCIAL NETWORKING

Employees are not permitted to access and browse social networking sites while on duty.

Employees are not permitted to post "selfies" of themselves on client property.

References to the Company must only be made on social networking sites following authorisation from the Company in advance only. References must be factual and favourable, Clients may not be mentioned by name.

Work related social networking site such as LinkedIn may be used to reference your employment with the Company. Details relating to your employment must be accurate. You must immediately update your working status should you change roles during your employment or in the event that you leave the Company.

Content can only be posted to the Company's social media accounts as the company by authorised Hackle personnel and media consultants. Any posts made to social media pages will be subject to approval by a page administrator.

TALKING TO THE MEDIA

Description

How to handle inquiries from any media such as newspaper, radio, TV, cable access, magazine, trade organisations, etc.

Background

Hackle Security Services Ltd strives to advance its mission by communicating openly and honestly using consistent messages with its constituents, including the media. It is important for all Hackle Security Services Ltd employees to reinforce these messages by referring all calls or emailed inquiries from any media source to the appropriate staff.

Procedure

To ensure the quality and consistency of information disseminated to media sources, the following policy shall be enforced:

- All media inquiries are to be handled by the Managing Director, regardless of who the media representative is, whom he or she represents, or how innocuous the request.
- All press releases or other promotional materials are to be approved by the Managing Director or his or her designee prior to dissemination.
- Please refer all calls or inquiries to the Company's Head Office, 020 7735 1955 or enquiries@hacklesecurity.co.uk; should you receive an emailed inquiry, please forward this to enquiries@hacklesecurity.co.uk, and do not reply to the sender.
- Please do ***not*** offer information to media — even if you know the answer. It is helpful for the Company that all news contacts be handled by senior staff and documented. Also, it's too easy to get quoted as an organization spokesperson if you volunteer something the reporter wants to use. In general, it is not advisable to say "no comment," since that constitutes a form of an answer that may be used against the Company in some instances and may lead to adverse publicity.

BREACHES OF THIS POLICY

Failure to comply with any aspect of this communications policy shall be grounds for disciplinary action.

1. Minor Breaches
Minor breaches of this policy shall constitute a disciplinary offence and will be dealt with using the disciplinary procedures of the Company.

2. Major Breaches

Major or serious breaches of this policy shall constitute gross misconduct and shall allow the Company to terminate your employment, immediately, without notice.

By signing this statement, it confirms that you have read and understood the Company Policy on Email and the Internet as set out above.

Officer:

Name: …… Signature: …….. Date: ……..

Line Manager:

Name: …… Signature: …….. Date: ……..