**Information Security, Internet, email and social media policy**

Introduction

This policy is:

- To make clear company policy on the internet and email use at work

- To protect individuals and the company against liability, security threats and any potential law breaking.

- To encourage our employees to use any social media positively and in line with company values and expectations.

General principles

Employees in carrying out their responsibilities are encouraged to use the internet and social media in ways that promote the goals, values and company objectives.

Work phones, IT systems, email accounts, computers, social media etc. are only to be used for communications and purposes approved by managers and in only accordance with company business.

Email and internet use on company equipment may be monitored for reasons associated with security and to ensure compliance with the Data Privacy regulations and Data Protection Act.

Employees may be asked to limit their use of and time on the internet and social media on company resources.

Information posted on the internet, social media and email is subject to the scrutiny of the senior management and the company reserves the right to decide if any information posted is suitable and in line with company ethos. Anything bringing the company into disrepute could lead to gross misconduct.

Illegal use will be reported in accordance with UK laws around IT use and social media posts and data protection and privacy.

Internet, email and social media use

Personnel are not to access, forward or post hateful, obscene, illegal, objectionable material or comments.

Employees are not to waste time on non-work activity during work hours on-line or on social media.

When communicating online, through social media or email with customers or other companies, ill-advised wording or comments that are not appropriate can

cause offence even if that is not the intention and damage the reputation of the company.

Employees are to seek advice from managers before responding in email or social media to complaints or negative comments from customers or the public and seek approval of wording before responding.

Information about any of our customers or other employees, or anything comedically sensitive must never be used on any social media – this could break UK data privacy laws and lead to gross misconduct.

Confidentiality including from company email addresses/social media

Employees are not to send company nicemove materials, upload or download nicemove materials or any information that is copyrighted by other companies without authorisation.

Do not share, post or send information to work or personnel accounts that is confidential to the business or linked to employees or customers – this includes any financial details, personal data and information, business ideas, public relations and marketing information, customer lists, door codes, passwords.

All personnel are to act in compliance with this policy and protect the privacy and confidentiality of other employees, all our customers and the reputation and interests of the company and any other companies we work with.

Any actions that are not in accordance with this policy and breach confidentiality or data privacy laws may be subject to disciplinary action including gross misconduct and dismissal.

Data protection – portable media

Any use of USB sticks, laptops, CD Roms, or other portable devices – compliance with company data protection and security should be observed, and permission always sought from management for recording or carrying any company data on such devices. Unlawful use or breaches in appropriate processing may be a disciplinary offence and .

Security

Company approved virus protection must be in place before any software or files are downloaded onto company devices.

Only authorised personnel can access or change usernames or email addresses or company files.

Password Rules and Guides

Please follow the advice below on creating an effective password of sufficient complexity for use on company accounts and devices: -

- At least 8 characters long.

- Do not use the name of a user or part of name over 2 letters.

- Always use a mix of uppercase, lowercase, numbers and symbols.

- Using the first letters of the words within a phrase you can remember is a good way to create a very secure, easy to remember password.

Password support:

- If you forget password – contact the warehouse office.

Using social media sites in the company’s name

All nicemove social media accounts are only accessible by senior management and office admin team and content is always the responsibility and under direction of senior management.

The company does not take responsibility for any content posted by third parties.

Any comments, complaints or questions from members of the public or customers on social media are always to be brought to the attention of the senior management team.

Use of social media

- Individuals are responsible for what content they post or upload and remember that it will be public and accessible for many years.

- Be mindful of how what you post could contribute to the reputation of the company.

- Don’t discuss the company, colleagues, competitors, customers or suppliers.

- Any member of staff who feels harassed, bullied, or offended by something posted or uploaded by a colleague onto a social media website should inform senior management.

- If you see any content posted on social media about the company (whether positive or negative), please report it to senior management team – do not respond directly.

- If you make a mistake in posting something on social media, quickly report, admit and correct it.

- If you feel even slightly unsure about a post, do not post, and when in doubt, always discuss it with your manager.

-

Monitoring use of social media

Staff should be aware that any use of social media websites (for work purposes) may be monitored and, where breaches of this policy are found, you will be asked to remove/adapt your profile or message, if necessary.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the company. It may also cause embarrassment to the company and to our clients.

In particular – to summarise - uploading, posting, forwarding or posting a link to any of the following summary below on a social media website, in a professional capacity, will amount to gross misconduct (this list is not exhaustive):

- Pornographic material

- A false and defamatory statement about anyone or a company/organisation;

- Material which is offensive, obscene, criminal, discriminatory, derogatory or may cause embarrassment.

- Any copyright or other intellectual property rights breaches, or which invades the privacy of any person.

- Confidential information about the company, any of our staff or clients.

- Any other statement which could create any liability (whether criminal or civil, and whether for you or us).

GDPR and storage of employee and customer data

All computers are password protected, and the office is coded entry.

Employee information and details are held in password protected files, and only used for contact, emergency and payment purposes. Information is not shared to any other personnel.

Handling of client data (such as addresses) – client information including addresses, names, payment information, invoices, are not to be printed or shared or used in any way other than necessary for duration of a job and for office accounting/invoicing purposes