INTRODUCTION

The Company acknowledges and accepts the widespread use of social media and other internet platforms by employees. However, the Company must ensure that client confidentiality or the reputation of the business is not compromised by the use of social media and other internet sites and therefore all employees are required to read and comply with this policy.

Representing the Company

Employees may indicate on their social media profiles etc. that they are an employee of the Company. However, no suggestion may be made by the employee that they represent the Company or the views of the Company on any social media or other internet site.

The employee may not seek to promote or market the Company in any way on a personal social media platform or internet site without the express authority of the Company.

An employee may not set up a social media profile or other internet site on behalf of the Company without the express authority of the Company unless to do so forms part of the employee's job description.

Computer and Data Protection

It is the Company's policy to comply with all laws regulating computers and data protection. It is therefore important that all employees minimise exposure to risk through careless practices with regard to the use of data or inappropriate, or illegal, use of software. Employees supplied with computer equipment are responsible for the safety and maintenance of that equipment and the security of software and data stored either on their own systems or other systems which they can access remotely.

Employees are only authorised to use systems and have access to information which is relevant to their job. An employee should neither seek information nor use systems outside of this criteria. Use of the internet is monitored and inappropriate activity will result in the Company taking disciplinary action.

Personal password should be kept confidential at all times and should never include personal data. Passwords should be changed regularly and must never be shared or divulged to any unauthorised person.

All employees are required to comply with all policy documents issued by the Company with regard to the use of computer equipment.

It is illegal to make copies of software. Software issued by the Company for your use is licensed to the Company and is protected by copyright law. You must not make or distribute software that has been copied.

Social media and internet content related to the Company

As a general rule Employees should refrain from making any comment about their employment or the Company, regardless of tone and context.

In particular employees must not make any comment or post any content on their social media profiles or other internet site which can be accessed by members of the public or clients of the Company and which could reasonably be considered to damage the reputation of the Company or any other employee, agent or contractor of the Company.

Employees have the opportunity to raise issues regarding their employment through the Company Grievance Policy and this is the proper course of action where they have a complaint.

Making comments or posting comments on a public profile or forum which may adversely affect the Company may result in formal disciplinary proceedings being commenced against the employee.

Social media and internet content related to clients of the Company

Employees must not, unless with the express authority of the Company, make a comment or post content on a social media or other internet site which discloses information relating to any client of the Company or the operations of the Company.

A failure of any employee to comply with this requirement may result in formal disciplinary proceedings being commenced against the employee.

Offensive comments or conduct

Where an employee has indicated that they are an employee of the Company on a social media or other internet site and that profile or site is accessible to members of the public or clients of the Company then the employee should refrain from making comments or posting content which could reasonably be considered to cause offence on the basis of race, nationality, gender, age, disability or sexual orientation.

Where the employee makes such comments or posts such content then the formal disciplinary proceedings may be taken against the employee where the Company considers that the comments or content could adversely affect the reputation of the Company.

Privacy Settings

It is recommended that employees ensure that they have appropriate privacy settings applied to their social media profiles where they have indicated that they are employed by the Company and may post comments or content of any form about the Company or any of its agents, employees or contractors.

Such privacy settings should limit access to the profile (or at least content relating to the Company) to your approved 'friends' or 'contacts' and not the public in general.

Internet Use

The internet is available for use on Company computers and other devices in order to assist employees in the performance of their job role. The internet should not be used during working hours for personal use, unless this is agreed with a line manager.

Employees may use the internet for personal use before and after working hours and whilst on a designated rest break. All use should be reasonable and no offensive, pornographic or other inappropriate internet access should be accessed.

The Company internet service is not to be used to download files for personal use such as music or video files as this will disrupt and slow down the internet connection for other users who are working.

The Company may restrict access to certain sites for all employees, or those who are found to have abused this privilege.
Abuse of the right to use the internet at work may result in formal disciplinary proceedings being commenced against an employee.

Monitoring

The Company respects the right of each employee to privacy and it is the preference of the Company that no monitoring should be required of an employee's email and internet use.

However, the Company reserves the right to monitor and review email and internet use where it is in the best interests of the business to do so, for example, to investigate performance and conduct issues or matters of public interest such as activity which is criminal or in breach of health and safety rules.

The Company will only monitor internet and email use in a proportionate manner and those persons carrying out the monitoring activities will be required to treat any information disclosed in the process as confidential.

Only information relating to the matter which has prompted the monitoring process will be obtained and stored unless information which the Company could not reasonably be expected to ignore is discovered, such as that which indicates a crime or breach of health and safety or company rules will is or has been committed.

Computers Designated for Student and Apprentice Use

Computers designated for training purposes are controlled by blocking any internet access or, where necessary, allowing limited internet access. Limited internet access is controlled by the IT department who instal localised localise PF Sense firewall devices with content filtering enabled to ensure that no extremist, unethical, sexual or radical material can be accessed. This also blocks social media access.

Approved/Authorised by:

Tim Armitt
Managing Director

Nicola Dodsley
Operations Director