



White and Company plc

Social Media Policy

(Version 1.3)

Revision History

REVISION	DATE OPERATIONAL	CEO/BOARD APPROVAL	NEXT REVIEW	PREPARED BY & COMMENTS
1.0	01/07/2017	01/07/2017	08/2019	Mr. S. Shahi – Group IT Manager Original
1.1	14/02/2020	14/08/2020	02/2023	Mr. S. Shahi – Group IT Manager Minor Change
1.2	01/07/2023	01/07/2023	07/2026	Mr. S. Shahi – Group IT Manager Minor Changes
1.3	03/08/2026	03/08/2026	08/2027	Reviewed



Introduction

Computer information systems and networks are an integral part of business at White and Company plc.

The company has made a substantial investment in human and financial resources to create these systems. The enclosed Policy and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the good name of the company.
- Protect our workforce.

Violations

Violations may result in disciplinary action in accordance with Company policy. Failure to observe these guidelines may result in disciplinary action by the Company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, or harm and distress to employees, and/or the presence of any repeated violation(s). Depending on the severity of the violation, once investigated it could lead to summary dismissal.

Administration

The Group IT Manager & Data Protection Officer are jointly responsible for the administration of this policy.

Social Networking

For the purpose of this Social Media Policy, 'Social Networking' covers Facebook, Twitter, YouTube, WhatsApp, LinkedIn, Instagram, TikTok, Flickr. This list is by no means exhaustive and this Policy may cover any website that has been classified by ISPs as a 'Social Networking Site'.

Employees Responsibilities

An employee who uses 'Social Networking' sites shall abide by the following:

- Proprietary information relating to the Company, Staff or Customers shall NOT be discussed or referred to on any social networking site without first obtaining the Company's express written permission to do so. Examples of information considered by the Company to be strictly off limits is financial, intellectual property and information relating to customers, although this list should not be deemed to be exhaustive.
- When employees sign up to any social networking sites, the Company holds employees responsible for reading, knowing and complying with all relevant Terms and Conditions of the relevant site(s) and all that entails and any repercussions which may result if the individual refers to its employer.
- Employees should never make defamatory comments about the Company, staff or customers at any time on any website.
- The use of Company equipment to access 'Social Networking' sites is strictly prohibited unless written consent has been obtained from management (Branch/Dept. Manager). Accessing such sites should never interfere with the employee's primary job responsibilities.
- Employee's using social networking sites that use the Company name should remember that, as a social networker, he or she also becomes, to some extent, a representative of the Company. Therefore, everything posted has the potential to reflect on the Company and its image. It should be noted that in such cases the individual must take on the responsibility for representing the Company in a professional manner and that under



no circumstances whatsoever, even in jest, should derogatory comments be made about the Company, its staff or its customers

- Employees are requested NOT to write recommendations or referrals for friends/associates on their chosen social site as a representative of the Company, as this may falsely give the appearance that the Company itself endorses the recommendation thus potentially creating a liability scenario for the company.

IT Manager's responsibilities

IT Manager shall:

- Install and maintain appropriate website filters to prevent access to 'Social Networking' Sites (unless agreed with the CEO and Dept./Branch Manager),
- Monitor and report such abuses to the CEO and DP/IT Teams.

The Data Protection Team's responsibilities

The DP Team shall:

- Responds to alleged violations of regulations, policies, procedures,
- Initiate any formal investigative procedure,
- Present the results of the investigation to relevant management,
- Take any relevant action required, after consultation with management, to address the violation in a proportionate manner,
- Monitor the offending target for compliance

Summary

Social media has a big part in society. We must ensure that the good name of White and Company plc is maintained. Do not post information or content that is false, misleading, defamatory, insinuating, abusive, harassing, threatening, discriminatory, obscene, or harmful to others.

Acknowledgement

By signing below, I agree to the following terms:

I have received and read a copy of the "Social Media Policy" and understand the same;

Employee Signature: _____

Employee Name: _____

Date: _____

Branch/Department: _____