Social Media Policy Statement

Social media is a huge phenomenon which has changed how many people communicate, reference companies, services and people, and interact. Websites, blogs and forums create public and private channels for third parties, networks, employees, competitors to access material and comment. Like it or not, social media can impact on personal and professional life – even though individuals and companies are not always able to post, edit or change what appears for others to consume. It is for this reason that WCS Group has a social media policy.

Introduction

Employees of WCS Group may be able to access social media services and social networking sites at work, either through company IT systems or via their own personal equipment. This Social Media Policy describes rules governing use of social media at WCS Group.

It sets out how staff must behave when using the company's social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff may say about the company on their personal accounts. This policy should be read in conjunction with employment contracts and employee service agreement.

The need for a social media policy

Social media brings significant benefits to the company – particularly for building relationships with clients and potential clients and suppliers / partners. However, social media needs to be used responsibly, ethically, honestly in a way that advances the company's vision, mission and values and does not damage its reputation or confidentiality of information. A social media policy is needed for employees to provide a framework for employees and to protect the company's operating capability and reputation.

Policy scope

This policy applies to all employees, contractors and volunteers at WCS Group who use social media while working – no matter for business or personal reasons. It applies no matter whether social media use takes place on a company site, while travelling for business or working from home. Social media sites and services of relevance may include but not be limited to -

- Popular social networking sites (Twitter, Facebook etc);
- Online review websites (Reevoo, Trustpilot etc);
- Sharing and discussion sites (Delicious, Reddit etc);
- Photographic social networks (Flickr, Instagram etc);
- Question and answer social networks (Quora, Yahoo Answers etc);
- Professional social networks (LinkedIn, Sunzu etc).

Responsibilities

Everyone who uses social media or uses a personal social media account at work, has some responsibility for the implementation and adherence to this policy. However, certain employees have particular responsibility: -

- Head of UK Sales and Marketing is ultimately responsible for ensuring WCS Group uses social media safely, appropriately and in line with the company's objectives;
- The Head of IT is responsible for providing apps and tools to manage the company's social media presence and track any key performance indicators;

- The Marketing Manager is responsible for working with colleagues to roll-out appropriate news and information responsibly where approved by senior management;
- The Customer Service Manager / Operations Head is responsible for ensuring requests for assistance and support made via social media are followed up.

General social media principles accepted

WCS Group believes that social media offers a potential platform for the company to perform marketing, stay connected with customers and potential customers and build or maintain an online presence. The company believes key staff should be involved in industry conversations on social networks and that social media is an excellent way for employees to make useful connections, share ideas and build relationships. Basic advice and parameters offered to employees include: -

- Know the social media – don't rush to comment or contribute;
- If unsure, don't post or comment or 'like';
- Be thoughtful and polite at all times;
- Look out for security threats;
- Keep personal use reasonable;
- Don't make business promises with checking and appropriate authorisation;
- Handle complex queries via other direct channels (company email, telephone, documented proposal etc);
- Don't escalate things;
- Don't intervene without consulting and seeking the backing and agreement of a line manager or senior management;
- Remember – all employees are officers of the company and expected to maintain the standards of etiquette, integrity and professionalism enshrined within the company's Vision, Mission and Values at all times;
- Social media for private use is perfectly alright provided employees respect sensible, described boundaries and expectations expressed in the Social Media Policy and employment contracts and HR policy which may change from time to time;
- If employees have a query, concern or worry, they must not hesitate to ask a line manager or senior manager.

Authorised users

Only employees who have been authorised to use the company's social networking accounts may do so. Authorisation is usually provided by senior management and documented. Restricted authorisation is the company's chosen way of maintaining a degree of consistency and control that is thought appropriate and prudent for sensible day to day operations.

Creating new social media accounts

Social media accounts may not be created without the written approval of a senior manager. The company operates a limited social media presence using the most appropriate industry networks where resources permit.

Purpose of company social media accounts

WCS Group's social media accounts may be used for different purposes. In general, employees may only post news approved in writing by a line manager or senior management – and then only news which is clearly in line with the company's overall business objectives.

For example, employees may use social media to: -

- Respond to a customer / potential customer request for help / initial enquiry;
- Share blog posts, articles and content that is approved for use in the public domain by authorised approvers;
- Share insight and articles that are relevant but have been penned by third parties;
- Provide fans or followers or potentially relevant parties with insight on what the company does;
- Promote marketing messages;
- Support new product or service launches – but only reaching out to relevant people.

Inappropriate content and use

Company social media accounts must not be used to share or spread inappropriate content, sensitive information, confidential data or take part in any activity which may bring the company or its operations in to question or disrepute. When sharing content, the author or poster must read and understand it thoroughly first and comply with Social Media Policy and standard Group employment terms.

Use of social media at work

The company permits employees to: -

- Make industry contacts at work who may be useful in their jobs;
- Discover content and information that may be useful in their job;
- Help to build company profile providing they have authority to do so.

Employees are not entitled to:

- Make public or private statements about the company on their personal web space;
- Make public or private comments about work which do not represent the company's views or opinions;
- Transmit, forward or link themselves to content about the company which may be defamatory or inappropriate (includes pornography, racial or religious slurs, gender-specific comments, information regarding criminal skills or terrorism or content that may be construed as harassment or corrupting for example);
- Use social media for criminal or illegal activities;
- Send, post or share messages that could damage the company's reputation;
- Discuss colleagues, customers or competitors or suppliers without their written approval;
- Post, forward, upload or link to spam, junk email, chain emails and messages.

Copyright

WCS Group respects, co-orperates and operates within copyright laws. Users may not use social media to: -

- Publish or share any copyrighted software, media or materials owned by third parties unless permitted by that third party and authorised by senior management;
- Share links to illegal music, films, games, video or software.

Employees may use share buttons or similar functions provided they adhere to the Social Media Policy.

Security and data protection

Employees should be aware of the security and data protection issues that can arise from using social media networks.

Users may not: -

- Share or link to any content or information owned by the company that is considered confidential or commercially sensitive (including but not limited to sales figures, key customer details and facts, future strategy, performance, pricing etc). For example, if a company's business intention was leaked on line, employees should not mention or point to it on social media;
- Share or link to data in any way that could breach the company's IT and Data Protection Policy.

Social media accounts should be protected via strong passwords that are changed regularly and only shared with authorised users.

Employees should watch and be vigilant for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the company or its customers. Employees are expected never to respond to or reveal customer information on social media platforms without authorisation.

Potential sanctions

Knowingly breaching this Social Media Policy is a serious offence because of potential risk – financial, operational, strategic, information security and reputation. Employees, contractors and other users may be held personally liable for violating this policy. Where appropriate, the company will involve the police and other law enforcement agencies in relation to breaches of this policy.

Mike Sullivan CBiol., MSB, MWM Soc
Managing Director