Social Media Acceptable Use Policy

DEFINITION

The Company: Refers to Nurture Fostering

PURPOSE

This policy is to be read and used in conjunction with the Security User: Responsibilities Policy.

The Company recognises that there are legitimate business and personal reasons for using social media at work and/or using corporate computing resources. To enable employees to take advantage of the business value of these sites and to promote an open, trusting, collaborative workplace, the Company policy allows all employees to use social media, but within the guidelines specified below. It is not possible to lay down rules to cover every possible situation. Instead, the policy is designed to set down general principles employees should apply when using electronic media and services. All such use should be done in a manner that does not negatively affect the use of the organisation's systems for business purposes.

WHAT IS SOCIAL MEDIA?

Social media includes any website or mobile application in which visitors are able to publish content to a larger group. Content shared may include (but is not limited to) personal information, opinions, research, commentary, video, pictures, or business information. Examples of such destinations include large branded entities such as Facebook, Twitter, YouTube, LinkedIn and other blogs and special interest forums.

General Use of Social Media

General use of social media is permitted for all employees, as long as such use is in accordance with the terms of this policy. All employees are expected to demonstrate a sense of responsibility and not abuse this privilege. Employees should not use the same password for all sites and must have different passwords for their personal and business personas.

Corporate Social Media Content

Posting of content to corporate sponsored social media (e.g. the corporate Facebook page) is permitted only for the marketing department who are authorized to publicly represent the Company.

INAPPROPRIATE CONTENT POLICY

While social media contains legitimate business and personal content, they also include content that is inappropriate for the workplace including nudity, violence, abused drugs, sex, and gambling. Therefore, the same inappropriate content policy that applies to the broader Web, also applies to content found within social media. Inappropriate content should not be accessed by employees while at work, or while using company resources. In addition to these guidelines, employees should use common sense and consideration for others in deciding which content is appropriate for the workplace.

The company employs technical controls to provide reminders, monitor, and enforce this policy.

PRODUCTIVITY POLICY

Social Media Acceptable Use Policy

The Company recognises that employees have a need, at times, to conduct personal business within social media while at work or using company resources. Therefore, the Company allows limited access to non-business social media content. For example, employees are allowed reasonable access to personal communications, email, and blog content within social media etc., if accessed in employees' own time.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

During non-business social media activity, employees must not publicly identify themselves as working for the Company, make reference to the Company or provide information from which others can ascertain the name of the Company.

It is the responsibility of the employee to ensure that personal business does not affect work quality or productivity. This policy is consistent with the Company productivity policy defined for the broader web outside of social media.

CONTENT PUBLISHING AND CONFIDENTIALITY POLICY

The following are policy indicators regarding what employees should and should not do when publishing content in social media. These indicators apply to all social media communications whether personal or company-sponsored.

Any employee that obtains electronic access to other organisations' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

An employee is legally responsible for content he or she publishes in social media and can be held personally liable for content, including any personal views they express. Defamatory statements can lead to lawsuits and adverse publicity. Any employee who publishes inappropriate or confidential content may be subject to disciplinary action by the Company. These indicators only cover a sample of all possible content publishing scenarios and are not a substitute for good judgment. If it would fail a good judgment test, then it is not allowed.

Policy Indicators

- Employees must not disclose or use the Company's confidential or proprietary information or that of any other person or company. For example, permission must be sought before posting fellow employee, customer or supplier pictures in a social network or publishing in a blog a conversation that was meant to be private.
- Employees must not comment on the Company's confidential financial information such as future business performance or business plans, or on any internal matters.
- Employees must not cite or reference customers, partners or suppliers without their written approval.
- Employees should identify themselves. Some individuals work anonymously, using pseudonyms or false screen names. The Company discourages such practice.
- Employees should be professional. If he or she has identified themselves as a Company employee within a social website, they are connected to their colleagues, Managers and even the Company's customers. Employees should ensure that content associated with them is consistent with their work and level of responsibility within the Company.

- Employees must obtain written permission to publish or report on conversations that are meant to be private or internal to the Company before doing so and when in doubt, should always ask permission from the Company Secretary, HR Director, Group HR Manager or an appropriate director.
- Employees should speak in the first person when engaging in personal social media communications. Make it clear that he or she is speaking for themselves and not on behalf of the Company.
- Employees should use a disclaimer, if an employee publishes personal social media communications and it has something to do with the work he or she does or subjects associated with the Company. An example of a suitable disclaimer is as follows: "The views, opinions and judgments expressed on this site are solely those of the author. The message contents have not been reviewed or approved by the Company and do not necessarily represent those of the Company."
- Employees should link back to the source. When employees make a reference to a customer, partner or supplier, where possible link back to the source.
- Employees should be aware of their association with Company social media – If he or she identifies themselves as a Company employee, he or she should ensure their profile and related content is consistent with how they wish to present themselves with colleagues and customers and is in accordance with this policy.
- Employees should use their best judgment. Remember that there are always consequences to what is published. Employees who are about to publish something that makes them even the slightest bit uncomfortable, should review the suggestions above and think about why that is. If he or she is still unsure, and it is related to Company business, the employee should discuss with their Manager or Director. If the employee does not have the benefit of such guidance, he or she should simply not publish it. Each employee has sole responsibility for what they post to their blog or publish in any form of social media.
- Employees must not use threatening, libelous, harassing content, neither must they use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable within the Company workplace. He or she must also show proper consideration for others' privacy and for topics that may be considered objectionable, inflammatory or defamatory.
- Employees must not conduct confidential business with a customer or partner business through their personal or other social media.
- Employees must not register accounts using the Company brand name or any other unregistered or registered trademarks without prior permission.

POLICY VIOLATION

Whilst the Company recognises the potential benefits of the many means of communication and information exchange afforded by using social media at work, employees should be aware that any abuse of the privilege of access to electronic media or services facilitated by the organization faces being subjected to disciplinary action, up to and including termination of employment, and risks having the privilege removed for themselves and possibly other employees.