SOCIAL MEDIA POLICY

Introduction

The growth in social media, particularly social networking sites has created increased opportunity for media communications that have an impact upon the business.

The term "social media" is used to describe dynamic and socially interactive network information and communication technologies, for example Web 2.0 sites, SMS text message and social networking sites such as Facebook, Snapchat, You Tube, LinkedIn, Twitter, blogs, other online journals and diaries, bulletin boards, chatrooms, micro blogging and the posting of videos on You Tube and similar media. Social networking also includes permitting or not removing postings by others where a player or employee can control the content of postings such as on a personal profile or blog.

This policy applies to social networking whilst both on and off duty.

The purpose of these social media guidelines is as follows:

- To encourage good practice
- To protect the business, its staff and clients.
- To clarify where and how existing policies and guidelines apply to social media.
- To promote effective and innovative use of social media as part of the business's activities.

General Guidelines

All current policies concerning staff apply to the use of social media these include, but are not limited to:

- Human resources: policies, procedures and codes of practice where applicable.
- Guidelines for the use of IT facilities.
- Data protection policies.
- Managing electronic mail and using e-mail wisely.
- Electronic information security policy and best practice in electronic information security.

Corporate Brand Guidelines

1. Staff should take effective precautions when utilising social networking sites to ensure their own personal safety and to protect against identity theft.

2. Staff who engage in social networking should be mindful that their postings, even if done off premises and while off duty, could have an adverse effect on the business's legitimate business interests, for example the information posted could be the business's confidential

business information. In addition some people who view this information may consider you as a spokesperson for the business. To reduce the likelihood that your networking will have an adverse effect on the business, staff should observe the following guidelines when social networking.

2.1. Staff should not engage in social networking by using any of the business's electronic resources or when they are supposed to be working.

2.2. Managers should not send "friend" requests to subordinates at any time while on or off duty.

2.3. Any member of staff may reject a "friend" request from any other member of staff without repercussion.

2.4. All requests for references or recommendations, even those that are received through social networking should be handled strictly in accordance with the business's standard policy for responding to such requests.

3. If the social networking of any member of staff includes any information relating to the business, the following must be adhered to:

3.1 It should be made clear to contacts and those who view social media that the views expressed are those of the member of staff alone and do not reflect the views of the business, by stating for example "the views expressed in this post are my own. They have not been reviewed or approved by the business".

3.2 The business's performance, products or services or the products or services of its sponsors, vendors or other businesses must not be discredited or defamed in any way. Customers, clients, business partners and suppliers must not be mentioned without the prior approval of the business's management team.

3.3 Inaccurate, distasteful or defamatory comments are prohibited. In addition, the use of, or the accessing of or the sending of offensive, obscene or indecent material is strictly prohibited.

3.4 The business's logo, trademark or proprietary graphics or any photographs of the business premises or products or those of any other team must not be used at any time.

3.5 Personal or contact information or photographs of any other member of staff or any Director or manager must not be posted or used at any time without permission.

3.6 The business has spent substantial time and resources building its reputation and goodwill. These are valuable and important corporate assets, which need to be enhanced and preserved. Before any member of staff engages in any social networking activity which identifies that member of staff as an employee of the business, or that identifies the business in any way, it should be considered whether the social networking activity is damaging the business's reputation or potentially could damage the business's reputation. If there is any doubt or any uncertainty, the member of staff should refrain from posting any information. Remember, a post lives forever! Staff must think before they type.

3.7 Any complaints about work should be resolved by speaking directly to your respective managers, rather than by posting complaints on the Internet through any method of social media. If any complaints or criticism of the business or other members of staff is posted on any method of social media, any comment that may be defamatory or

damaging to the business or any other employees should be avoided. REMEMBER - Disciplinary action can be taken for this activity.

3.8 Social networking sites are prime targets for malware distribution, and third-party applications should never be downloaded.

3.9 Any incidences of inappropriate behaviour, information posting, phishing or suspected malware should be reported immediately to the business' Management team.

4. The business reserves the right at all times to continually review the use of social media and may modify its policies should the status of particular social media sites change, for example of charges are introduced or changes made to the way content is used or the terms of use of sites are changed or if a site closes down.

5. The business will in its sole discretion review the social networking activities of any member of its staff. This policy applies even if the social networking activity of any member of staff is anonymous or under a pseudonym. If such networking activity is engaged in, members of staff should be aware that in appropriate circumstances the business will take steps to determine the identity of the individual concerned.

6. The business may request in its sole and absolute discretion that any member of staff should temporarily confine their respective social networking activities to matters unrelated to the business if the business determines that it is necessary or advisable to ensure compliance with regulations or other laws.

7. If clarification is required on any aspect of this policy, members of staff should contact the business's management team. All members of staff should note that failure to comply with any aspect of this policy may lead to disciplinary up to and including termination, and if appropriate the business will pursue all available legal remedies to protect its reputation, produces, logo, trademark or proprietary graphics. The business reserves the right in addition to report any suspected unlawful conduct to the appropriate law enforcement authority.