Social Media Definition

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It also covers video and image sharing websites such as YouTube as well as blogs.**This policy applies to any social media that employees may use.**

Use of Social Media at Work

Employees must limit their use of social media to outside normal working hours and this **must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity**.

If employees see or hear about any inaccurate information about the company, this should be reported to their line manager.

Business contacts made through social media while employed amount to confidential information and the company may ask for them to be deleted from accounts at the end of employment.

Stambridge Social Media

Where employees are authorised to contribute to the company's social media activities as part of their job duties, for example for marketing, promotional and recruitment purposes, they must follow these rules:

- Use the same safeguards as they would with any other type of communication about the company that is in the public arena.
- Ensure that any communication has a purpose and a benefit for the company.
- Obtain permission from their line manager before embarking on a public campaign using social media.
- Request their line manager to check and approve content before it is published online.
- Follow any additional guidelines given by the company from time to time.
- The social media rules set out below also apply as appropriate.

Use of Social Media for Personal Use

Employees can still cause damage to the company if they are recognised online as being one of its employees. Therefore, it is important that the company has strict social media rules in place to protect its position. 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. This includes using work email addresses, providing links to company websites, writing about work, disclosing trade secrets, making damaging remarks about the company and its employees, giving personal information about staff (this could be a criminal offence under the 1998 Data Protection Act).

- Ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of the company.

- Conduct themselves in a way that is potentially detrimental to the company or brings the company or its employees, clients, customers, contractors or suppliers into disrepute. For example by posting images or video clips that are inappropriate or links to inappropriate website content.

- Allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the company, for example by criticising or arguing with such persons.

- Make any comments about the company's employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying – employees can be personally liable for their actions under the legislation.

- Breach copyright or any other proprietary interest belonging to the company. If employees wish to post images or videos of colleagues or clients, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by Stambridge Security Services Ltd.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by setting their privacy settings at a high level and restricting the amount of personal information they give out, such as date and place of birth, schools attended, family names and favourite football team. This information may form the basis of security questions and/or passwords on other websites, such as online banking.

Social Media References

Where employees (or ex-employees) have set up personal profiles on business networking websites such as LinkedIn, these websites may allow the user to request or provide open recommendations, endorsements or references.

As these could potentially be construed as open references given on behalf of Stambridge Security Services Ltd, employees are prohibited from providing these types of recommendations. Employees should refer such requests to their line managers.

Social Media Monitoring

Stambridge Security Services Ltd reserves the right to monitor employees' use of social media, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- Promote productivity and efficiency.
- Ensure the security of the system and its effective operation.
- Ensure there is no unauthorised use of the company's time.
- Ensure that all employees are being treated with respect and dignity at work.
- Ensure there is no breach of commercial confidentiality.

The company reserves the right to restrict, deny or remove access to any employee.

Contravention of This Policy

Failure to comply with this policy is a disciplinary offence and may result in disciplinary action. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.