SOCIAL MEDIA POLICY

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 includes social and business networking websites such as Facebook, MySpace, Bebo, Twitter and LinkedIn. Social media also covers video and image sharing websites such as YouTube and Flickr, as well as personal blogs. This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive. This policy applies in relation to any social media that employees may use.

USE OF SOCIAL MEDIA AT WORK

Employees are only permitted to log on to social media websites using the Company's IT systems and equipment outside their normal working hours (e.g. during lunch breaks or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. This includes laptop and hand-held devices distributed by the Company for work purposes. Grafters Recruit Ltd. nevertheless reserves the right to restrict or deny access to these types of websites at any time.

However, employees may be asked to contribute to the Company's own social media activities during normal working hours, for example by writing Company blogs or advertisements or newsfeeds, managing a Facebook account or running an official Twitter or LinkedIn account for the Company. Employees must be aware at all times that, while contributing to the Company's social media activities, they are representing Grafters Recruit Ltd. Contract Services Limited.

COMPANY'S SOCIAL MEDIA ACTIVITIES

Where employees are authorised to contribute to Grafters Recruit Ltd. own social media activities as part of their work, for example for marketing, promotion

The Company recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Company in these circumstances, employees must be aware that they 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.

When logging on to and using social media websites and blogs at any time, including personal use on non-company computers outside the workplace and outside normal working hours, employees must not:

- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, 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

- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, write about their work for the Company – and, in postings that could be linked to the Company, they must also 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 clients or its workers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content

- Other than in relation to the Company's own social media activities or other than where expressly permitted by the Company on business networking websites such as LinkedIn, use their work e-mail address when registering on such sites or provide any link to the Company's website

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

- Include personal information or data about the Company's employees and clients without their express consent (an employee may still be liable even if employees or clients are not expressly named in the

websites or blogs as long as the Company reasonably believes they are identifiable) – this could constitute a breach of the Data Protection Act 1998 which is a criminal offence

- Make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the Company, its employees or clients (an employee may still be liable even if employees or clients are not expressly named in the websites or blogs as long as the Company reasonably believes they are identifiable).

- Make any comments about the Company's employees that could constitute unlawful discrimination, harassment or bullying contrary to the Equality Act 2010 – you can be personally liable for your actions under the legislation.

- Revealing confidential information about Grafters Recruit Ltd. in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions

Employees should remember that social networking websites are a public forum, even if they have set their account settings at a restricted access or "friends only" level and therefore they should not assume that their entries on any website will remain private.

Employees must also be security conscious when using social networking websites and should take appropriate steps to protect themselves from identity theft, for example by 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.

Employees who are discovered contravening these rules, whether inside or outside the workplace, may face serious disciplinary action under the Company's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

All company employees or temporary staff who have been granted the right to use the company's internet access to log on to social and business networking websites are required to sign this agreement confirming their understanding and acceptance of this policy.

SIGNED:

……

PRINT NAME:

……

DATE:

……