

|  |
| --- |
| Firms Logo |
| SOCIAL MEDIA POLICY |
|  |
|  |
|  |

Amendments to this Policy

From time to time this policy will be updated to reflect changes [Specific\_Firm’s\_Name] regulated business (trading as [Trading\_Name]) or changes to the regulations to which [Trading\_Name] is subject. The Compliance Officer will ensure that all appropriate amendments are made to this manual, and this will be overseen by the Board. The dates of the amendments are recorded below. Please ensure that you have the most up-to-date version of this manual by confirming the correct version number with the Compliance Manger/CEO.

Instructions: Do not state “*Final*” as by definition policies are regularly reviewed.

Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Status** | **Date** | **Notes** | **By Whom** |
| 0.1 | Draft | 02/04/16 | For Application | Compliance Consultant |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Document Governance

|  |  |
| --- | --- |
| Policy Owner | TITLE |
| Approver | Board of Directors |
| Date approved | MONTH 20XX |
| Date last reviewed | MONTH 20XX |
| Review frequency | Annual |
| Next review date | MONTH 20XX |
| Responsible for document management | TITLE |
| Security classification | Restricted |

Contents

[**Social Media definition** 5](#_Toc451543645)

[**Social Media definition** 5](#_Toc451543646)

[This policy aims to provide protection and safeguarding for the firm’s reputation 5](#_Toc451543647)

[**Social Media Scope** 5](#_Toc451543648)

[**Use of social media at work** *(select option for you – amend as appropriate)* 5](#_Toc451543649)

[**Company’s Social Media activities** 6](#_Toc451543650)

[**Social Media rules** 7](#_Toc451543651)

[**Social Media references** 9](#_Toc451543652)

[**Social Media monitoring** 9](#_Toc451543653)

[**Contravention of this policy** 9](#_Toc451543654)

[Sources of reference used in collating this policy are; 11](#_Toc451543655)

[Further information 11](#_Toc451543656)

[Related Pages 11](#_Toc451543657)

[Other Sites 11](#_Toc451543658)

# **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 includes social and business networking websites such as, but not limited to, Facebook, MySpace, Bebo, Twitter and LinkedIn. Social media also covers video and image sharing websites such as, but not limited to, YouTube and Flickr, as well as personal weblogs (“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.

# **Social Media Policy Aim**

This policy aims to provide protection and safeguarding for the firm’s reputation and employees rights and freedoms. By raising awareness of the firm’s views regarding any comments made about the firm’s employees that could constitute or lead to consequences, intended or not, of unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 every employee is assured protection. Additionally, any post, images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying will be dealt with appropriately by the firm and it is thereby clear to all employees that they can be personally liable for their actions under the legislation.

# **Social Media Scope**

This policy applies to all employees, contractors, temporary or interim appointments, directors, and any other person that may conduct roles or provide services to the firm for any period.

# **Use of social media at work** *(select option for you – amend as appropriate)*

*Option 1 – Ban on social media use at work*

[Employees are not permitted to log on to social media websites or to keep a personal weblog (“blog”) using the Company’s IT systems and equipment at any time. This includes laptop and hand-held computers or devices distributed by the Company for work purposes. The Company has added most of the websites of this type to its list of restricted websites. Where employees have their own computers or devices, such as laptops and hand-held devices, they must limit their use of social media on their own equipment to outside their normal working hours (for example, during lunch breaks).

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 newsfeeds or 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 the Company.]

OR

*Option 2 – Limited social media use at work*

[Employees are only permitted to log on to social media websites or to keep a personal weblog (“blog”) using the Company’s IT systems and equipment outside their normal working hours (for example, during lunch breaks or before the working day has started 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 computers or devices distributed by the Company for work purposes. The Company nevertheless reserves the right to restrict access to any of these types of websites at any time. Where employees have their own computers or devices, such as laptops and hand-held devices, again they must limit their use of social media on their own equipment to outside their normal working hours.

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 newsfeeds or 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 the Company.]

OR

*Option 3 – Open social media use at work*

[The Company permits employees to make reasonable and appropriate use of social media websites or to keep a personal weblog (“blog”) using the Company’s IT systems and equipment or their own computers or devices, such as laptops and hand-held devices, during their normal working hours, provided this does not significantly interfere with their job duties or have a detrimental effect on their productivity. Employees must not spend an excessive amount of time while at work accessing social media websites. No more than [15 minutes] per day spent on social media websites during normal working hours is deemed acceptable.

Employees may also be asked to contribute to the Company’s own social media activities during normal working hours, for example by writing Company blogs or newsfeeds or 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 the Company.]

# **Company’s Social Media activities**

Where employees are authorised to contribute to the Company’s own social media activities as part of their job duties, for example for marketing, promotional and recruitment purposes, they must adhere to the following 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.
* Any page that is created containing references to the company directly or details of any person associated with that page working for the company will need to be cleared with compliance and operations.

The social media rules set out below also apply as appropriate.

# **Social Media rules**

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.

Under English law, if any member of staff has a grievance or other concern, there is a procedure to be followed in the staff handbook, compliance manual or by discussing the issue with HR. There are also “Whistle-blower” procedures available for appropriate reporting under those prescribed circumstances.

Damaging reputational consequences can be created by flippant or unguarded comments, even if meant with the best of intentions. As with most written mediums, (as many social media platforms are text based) these conversations are required to be stored by the provider and recalled by legal sequestering in case of misdemeanours, even if used out of context by the recipients in the conversation. Screenshots of text/chat boxes can be stored without your knowledge. Similar to the Electronic Communications Policy; “*if you don’t want it read, don’t write it*.”

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 for 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 deduce or 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 for 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 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.
* Other than in relation to the Company’s own social media activities or other than where expressly permitted by the Company for 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, customers, contractors or suppliers of the Company, for example by criticising or arguing with such persons.
* Include personal information or data about the Company’s employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers 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, adverse, discriminatory, untrue, negative, critical or defamatory comments about the Company, its employees, clients, customers, contractors or suppliers, or any comments which might reasonably be considered to insult, damage or impugn the Company’s or their reputation or character (an employee may still be liable even if the Company, its employees, clients, customers, contractors or suppliers 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 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.
* Disclose any trade secrets or confidential, proprietary or sensitive information belonging to the Company, its employees, clients, customers, contractors or suppliers or any information which could be used by one or more of the Company’s competitors, for example information about the Company’s work, its products and services, technical developments, deals that it is doing, future business plans and staff morale.
* Breach copyright or any other proprietary interest belonging to the Company, for example, using someone else’s images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work – if employees wish to post images, photographs or videos of their work 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 the Company.

Work and business contacts made during the course of employment through social media websites and which are added to personal social networking accounts amount to confidential information belonging to the Company and accordingly the Company may ask for them to be surrendered on termination of employment.

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

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.

Should employees observe inaccurate information about the Company on any web sources of information, they should report this to their line manager in the first instance.

# **Social Media references**

Where employees (or ex-employees) have set up personal profiles on business networking websites such as LinkedIn, these websites may include the facility for the user to request their contacts or other users to provide them with open recommendations, endorsements or references which are then published on their personal profile web pages for other contacts or connections, or prospective contacts or connections, to read. As these could potentially be construed as open references given on behalf of the Company, employees are prohibited from providing these types of recommendations, endorsements or references online to or for the benefit of other employees or ex-employees without the prior permission of their line manager.

If these types of recommendations, endorsements or references are requested online by clients, customers, contractors, suppliers or other Company-related business connections, employees should refer such requests to their line managers.

# **Social Media monitoring**

The Company reserves the right to monitor employees’ use of social media on the internet, 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, for example to check that an employee has not been spending an excessive amount of time using social media websites for non-work related activity when they should be working.
* Ensure that inappropriate, restricted or blocked websites are not being accessed by employees.
* Ensure that all employees are being treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to harassment contrary to the Equality Act 2010.
* Ensure there is no breach of commercial confidentiality.

The Company reserves the right to restrict, deny or remove internet access, or access to particular social media websites, to or from any employee.

By accepting this policy, you thereby agree, whether or not, when posting on any site on behalf of the firm:

* To set your Social Networking sites to Private so that only individuals that I approve may see the content of my site.
* Never to upload any inappropriate material (videos, photos, music, etc) that could damage the reputation of the firm.
* Not upload any material (videos, photos, music, etc) of “Staff”, “Employees” or “firm’s premises” (internal or external) or any material that identifies me as a firm staff member without the express permission of the Chief Operating Officer or Head of Human Resources.
* Not to accept “customers”, “clients”, “colleagues” or any person as “Friends” on the company or personal accounts, as they may then have unlimited access to my site.
* I will report any and all inappropriate internet use of the firm’s network to the appropriate Head of Department.

# **Contravention of this policy**

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken 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.

# Sources of reference used in collating this policy are;

**Legal considerations**

* **The Human Rights Act 1998** gives a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers, and all courts must interpret other existing legislation in relation to the Human Rights Act. Case law suggests that employees have a reasonable expectation of privacy in the workplace.
* **The Regulation of Investigatory Powers Act 2000** covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system. It applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications. There are two areas where monitoring is not unlawful:
  + Where the employer reasonably believes that the sender and intended recipient have consented to the interception;
  + Without consent, the employer may monitor in certain circumstances -for example, to prevent crime, protect the business or to comply with financial regulations.
* **The Data Protection Act 1988** covers how information about employees and job applicants can be collected, handled and used. The Information Commissioner's Office has published an employment practices code - [**Information Commissioner’s Office: Quick guide to the employment practices code [PDF, 168kb]**](http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/quick_guide_to_the_employment_practices_code.pdf) - to help employers comply with the law.

## Further information

### Related Pages

* [**Social media**](http://www.acas.org.uk/index.aspx?articleid=3375)
* [**Social media and managing performance**](http://www.acas.org.uk/index.aspx?articleid=3376)
* [**Social media and recruitment**](http://www.acas.org.uk/index.aspx?articleid=3377)
* [**Social media, discipline and grievances**](http://www.acas.org.uk/index.aspx?articleid=3378)
* [**Social media and bullying**](http://www.acas.org.uk/index.aspx?articleid=3379)
* [**Social media, defamation, data protection and privacy**](http://www.acas.org.uk/index.aspx?articleid=3380)
* [**Social media research paper**](http://www.acas.org.uk/index.aspx?articleid=4076)
* [**Social media - Acas training and support**](http://www.acas.org.uk/index.aspx?articleid=4077)
* [**Advisory booklet - Employee communications and consultation**](http://www.acas.org.uk/index.aspx?articleid=663)
* [**Discipline and grievances at work: The Acas guide**](http://www.acas.org.uk/index.aspx?articleid=2179)

### Other Sites

* [**Information Commissioner's Office**](https://ico.org.uk/)
* [**Intellectual Property Office**](http://www.ipo.gov.uk/)