*\*\*BLUE TEXT SHOULD BE REMOVED BEFORE ISSUE\*\**

***Social media policy***

*Use the social media policy to set out your rules on employees accessing social media websites during work time. Whilst you can’t prohibit employees accessing such sites in their own time using their own equipment, such as on their tablets and smartphones, you can try to ensure they don’t adversely damage your reputation, affect your client relationships or expose you to legal liability.*

**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 Facebook, Reddit, Twitter and LinkedIn. Social media also covers video and image sharing and blogging websites such as YouTube, Instagram, Snapchat, TikTok, Tumblr and Flickr, as well as personal blogs, any posts made on other people’s blogs and all online forums and noticeboards. 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**

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

[Employees are not permitted to access social media websites or to keep a 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 personal devices such as smartphones, they must limit their use of social media on this 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, 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 and they must not post any personal content on any Company social media account that they are authorised to use.]

OR

*Option 2 – Limited social media use at work*

[Employees are only permitted to log on to social media websites or to keep a blog using the Company’s IT systems and equipment outside their normal working hours (for example, 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 computers or devices distributed by the Company for work purposes. The Company nevertheless reserves the right to restrict access to this type of websites at any time. Where employees have their own computers or devices, such as laptops and hand-held personal devices such as smartphones, again they must limit their use of social media on this 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, 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 and they must not post any personal content on any Company social media account that they are authorised to use.]

OR

*Option 3 – Open social media use at work*

[The Company permits employees to make reasonable, professional and appropriate use of social media websites or to keep a blog using the Company’s IT systems and equipment or their own computers or devices, such as laptops and hand-held personal devices such as smartphones, during their normal working hours, provided this does not significantly interfere with their job duties or have a detrimental effect on their productivity and is in accordance with the terms of this policy. Employees must not spend an excessive amount of time while at work accessing social media websites. [No more than ……… *(insert figure)* minutes per day spent on social media websites 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, 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 and they must not post any personal content on any Company social media account that they are authorised to use.]

## Company’s social media activities

Where employees are authorised to contribute to the Company’s own social media activities as part of their work, 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 domain
* 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
* not under any circumstances post any personal content or express any personal opinions that do not represent those of the Company
* follow any additional guidelines given by the Company from time to time.

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

In addition, such social media accounts which are operated for business purposes (and their contents) belong to the Company and therefore these accounts used by an employee during employment may not be used after termination of employment. The Company may also ask the employee to supply their usernames and passwords either on termination of employment or at any other time and in either case the employee must supply them on request.

## 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. 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:

* use social media in a way that breaches any of the Company’s other policies - if an internet post would breach any of these policies in another forum, it will also breach them in an online forum
* 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 (and in any event they must not hold themselves out as associated with the Company on any social media website after termination of employment, which means any references to the Company, and their job role in the Company, must be removed immediately on employment termination)
* 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 and opinions expressed are clearly stated to be theirs alone and do not represent those of the Company
* create a social media account that could be mistaken for a Company social media account
* create a social media account or profile that impersonates one or more of the Company’s employees, clients, customers, contractors or suppliers
* use the Company’s logos, trademarks or other corporate artwork on a personal social media account
* conduct themselves in a way that is potentially detrimental to the Company or directly or indirectly brings the Company or its clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content or sharing inappropriate content posted by others
* 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 email 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 or using abusive or threatening language towards them
* 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 2018 which is a criminal offence
* make any derogatory, offensive, discriminatory, disrespectful, untrue, negative, misleading, critical, disparaging or defamatory comments or statements about the Company, its employees, clients, customers, contractors or suppliers (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)
* air grievances about the Company or any of its activities
* make any comments about the Company’s employees that could constitute unlawful discrimination, harassment, victimisation 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
* provide references for other individuals on social media websites, as such references could be attributed to the Company and create legal liability for both the author of the reference and the Company
* 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, current or future trading performance, deals that it is doing or future business plans, staff morale and anything else that is not already in the public domain
* 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, personal details 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 social media 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 (such as the names and contact details of existing or prospective customers, clients and suppliers) and which are added to personal social and business networking accounts (in particular to LinkedIn), or which are stored on the Company’s computer system, amount to confidential information belonging to the Company and accordingly must be surrendered when requested and on termination of employment.

On termination of employment or once notice to terminate employment has been given, employees must, on request, disclose to the Company a full list of all work and business contacts that they hold on all devices or on all social and business networking accounts. The Company may then require the departing employee to delete any or all such work and business connections from their devices (including from personal devices) or from their social or business networking account, not keep copies of the same and not reconnect with those connections for a period of six months from termination of employment. The Company may also require written confirmation from the employee that these provisions have been complied with.

Employees must also surrender all login and password details for accounts run on the Company's behalf or where an account has been used to promote and/or market the Company's business activities on the termination of employment or whenever so requested by the Company.

Employees should remember that social media websites are public fora, 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 postings on any website will remain private.

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 placing their privacy settings at a high level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

Should employees notice any inaccurate information about the Company online or which breaches this policy or otherwise brings the Company into disrepute, they should report this to their line manager in the first instance.

Employees are not permitted to use private email, text messaging, messaging apps or any other instant messaging or chat programs or services to discuss work-related matters or for any other business purposes – employees must always use the Company’s official correspondence channels for work-related business and must never use such private correspondence channels.

## Social media monitoring

The Company reserves the right to monitor employees’ use of social media on the internet, both during routine audits or random spot checks of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

The Company will only monitor use of social media on the internet where we have a lawful basis for doing so. The business purposes for such monitoring are to:

* establish the existence of facts
* ascertain compliance with regulatory or self-regulatory requirements, practices or procedures
* assess standards of employee performance and conduct and promote productivity and efficiency
* investigate or detect any unauthorised use of the systems
* ensure the security of the systems and networks and their effective operation
* ensure the smooth running of the business by checking whether there are any relevant business communications that need to be dealt with
* ensure that the Company’s rules, policies and procedures are being complied with
* record transactions
* promote client and customer satisfaction
* ensure that the systems are not being used for any unlawful purpose or activities that may damage the Company’s business or reputation
* make sure there is no unauthorised use of the Company’s time
* perform effective internal administration
* ensure that inappropriate, restricted or blocked websites are not being accessed and that offensive or illegal material is not being viewed, sent, downloaded or circulated
* ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
* protect the privacy of personal data, trade secrets and sensitive or confidential Company information and ensure there is no breach of confidentiality or data protection provisions.

Members of the IT department are authorised to monitor social media on the internet during routine audits or random spot checks and they may also be instructed to do so by managers where a problem is suspected. Access to the results of monitoring is restricted to the IT department and to those managers who are authorised to access them in accordance with the purposes outlined above. Disclosure of the results of monitoring to other third parties will only be made in accordance with the purposes outlined above and will be limited to:

* the police and other law enforcement agencies, where the results could assist in the prevention or detection of a crime or the identification and prosecution of an offender
* prosecution agencies, such as the Crown Prosecution Service
* relevant legal representatives
* managers involved with Company disciplinary and performance management processes.

The Managing Director (or another senior director acting in their absence) is the only person who is permitted to authorise disclosure of information to external third parties such as law enforcement agencies.

Social media monitoring may involve obtaining an itemised log of all social media websites and individual web pages visited, as well as the date and time of access. Where the particular circumstances warrant it, it may also involve accessing the actual content posted or circulated on social media web pages.

The Company is committed to being transparent about how and why employees are monitored and will always consider whether the monitoring measures are proportionate.

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

#### Contravention of this policy

Failure to comply with any of the requirements of this policy, including failing to remove any social media content that in itself breaches 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. Any employee suspected of committing a breach of this policy will be required to co-operate with the investigation, which may involve handing over relevant login and password details.

In addition, employees could face legal proceedings if comments they post about the Company or named individuals are found to have harmed their reputation.