Social Media policy

Date reviewed: January 2021
Date next reviewed: 21 January 2022

Introduction

The Participation People's Social Media Policy aims to ensure employees are familiar with and understand the implications, consequences and risks associated with the use of social media when disclosing information and posting comments associated with the Company, our clients, suppliers and employees. This policy covers the use of all forms of social media including Facebook, LinkedIn, Twitter, Wikipedia, YouTube, Instagram and all other social networking websites, online review websites, sharing and discussions sites, photographic social networks, as well as any other postings/blogs on the internet.

This policy applies to all employees and other workers within the Participation People, whether full time or part time as well as agency workers, temporary workers, contractors and also third parties who have access to our computers, networks or other electronic communication systems or equipment.

Policy

This policy outlines your responsibilities when accessing social networking websites during and outside of working hours, for private or business purposes, from computer, mobile phone or electronic communication systems, networks and equipment belonging to you, the Company or others.

This Social Media Policy aims to increase your awareness of the risks to the Company's reputation with regards to the accessing and posting of comments and photographs on social networking and internet sites as well as ensuring compliance of confidential and proprietary information policies. It also identifies legal obligations so that you understand your responsibility in preventing or minimising risks to the Company. In setting and monitoring these standards, we will comply with your individual rights and any further legislative requirements.

Employees should be aware that breaching this policy may result in disciplinary action up to and including dismissal in line with the Company's Disciplinary Procedure. If you are

suspected of breaching this policy, you will be required to co-operate fully with our investigation and you may be required to provide relevant passwords and login details to the internet sites to enable us to undertake a full and fair investigation and you may be required to provide relevant passwords and login details to internet sites to enable us to undertake a full and fair investigation. Any internet posting that is deemed to constitute a breach of this policy may result in a request being made to remove it. Failure to comply with any such request may result in disciplinary action being taken.

This policy may be amended from time to time.

Monitoring

The content of the Company's electronic communication systems and equipment are the property of the Company. You should be aware that there is no expectation of privacy in any document, file, message, fax, telephone conversation, social media post, data or message of any other kind of communication or information transmitted to, received or printed from, stored or recorded on our electronic communications systems and equipment.

Company electronic communications systems and equipment should not be used for any matter that you wish to be kept private or confidential from the Company.
As referred to in your terms and conditions of employment, the Company reserves the right to access, monitor, intercept, retrieve and review all use of the internet including social media postings and activities using our electronic systems, network and equipment. Any such monitoring will be to ensure that our rules are being complied with and for legitimate business purposes, such as ensuring network and information security and/or disciplinary and/or performance review purposes. Any monitoring shall be carried out in accordance with the Company's IT & Communications and Data Protection policies.
We may store copies of such data or communications, including social media postings, for a period of time after they are created, and may delete such copies without further notice. Information will not be stored for longer than is necessary, for the purposes set out above, and shall be retained and deleted in accordance with our employee privacy notice and/or data retention policy.

Use of Social Media

A certain reasonable amount of personal use of the email and internet system is permitted by the Company, provided that this is compliant with this policy and does not interfere with your employment responsibilities or productivity. However, access to social networking websites or personal email accounts (Hotmail, Yahoo etc.) from its computers, networks and other electronic systems and equipment including mobile phones and PDA's is only permitted during unpaid break times.

The Company reserves the right to restrict access to social media websites at any time during or outside of working hours on our electronic communication systems.
Employees must not use social media or any other form of online messaging platform to:

- Breach any Company policy, including its Data Protection Policy and any associated privacy notices
- Breach any confidentiality obligations (including, without limitation, posting, sharing or linking to any content or information owned by the company that could be considered confidential or commercially sensitive or proprietary information or commenting about business-related topics such as performance without first obtaining written permission from your manager)
- Breach any other obligations under any employment contract
- Breach the Company's disciplinary rules
- Breach the Company's ethics and standards of conduct
- Breach any other laws or regulatory requirements
- Disparage or defame the Company, our clients, suppliers, all other affiliates and stakeholders or any third party with whom we have dealings
- Post comments which could be misinterpreted so as to directly or indirectly damage our reputation as a Company and employer
- Post any false or misleading statements about the Company, our management team, or our employees (present, past or prospective), our clients, suppliers, all other affiliates and stakeholders or any third party
- Post any discriminatory, insulting, obscene, harassing or offensive comments relating to colleagues, our clients, business partners, suppliers or any other third parties
- Post any other comments relating to colleagues, our clients, business partners, suppliers or any other third parties without their written permission
- Post any valuable trade secrets, other confidential information and intellectual property of the Company regardless of whether or not the integrity of such information would be jeopardised
- Misappropriate or infringe the intellectual property or confidentiality of other companies or individuals, which can create liability for the Company and/or for yourself individually; as the author
- Create any social media account in the Company's name unless authorised in writing by your manager
- Use Company logos, brand names, slogans or other trademarks
- Set up any spoof or serious fan pages, videos, Twitter or Instagram accounts or Facebook pages in the Participation People's name
- Bully, victimise, make unwanted contact with or impersonate another member of staff, client, supplier or other third part in any form
- Express opinions about or on behalf of the Company via social media, unless authorised in writing by your manager.

This list is intended as a guide and is not exhaustive.

Employees must not provide references for other individuals on social networking sites as they can create legal liability for both the author and the Company.

Responsible Use & Reputation

All employees of the Participation People are personally responsible for what they write on any social networking or internet site. You should therefore be aware that these sites are public forums and ‘networks’ and as such, whatever is written on them may be available to the public including the Participation People, future employees and social contacts for a long period of time.

You should remain professional in what you post and in the image that you portray in your profile. Reference to the Company should be avoided and this includes the posting of business sensitive topics such as how the business is doing or clients we are working with. It should be made clear that you are speaking on your own behalf.

With the exception of LinkedIn, if you access and use any type of social networking site you should use a personal e-mail address in any other communications that you make on these sites. You may, with the Company’s permission, use Company email addresses on LinkedIn for business purposes only.

All employees are responsible for protecting the Company’s reputation. You should therefore inform the Chief Executive Officer as soon as reasonably practical should you come across any comments that disparage the Company, our suppliers, clients or other employees or otherwise exposes the Company to liability.

Confidential and Proprietary Information

During employment, employees develop business contacts and also friends through social networking sites. This may be with encouragement and approval from the Company and could include networking with clients and competitors. Sharing contacts means that competitors of the Company can access client’s details and as such contact our clients, which could potentially result in a loss of business for us. With this in mind, we would ask that you ensure your privacy settings on such sites are set at an appropriate level to reduce this risk.

The Participation People considers that any business contacts developed or obtained by you during your period of employment to be the property of the Company. The Company reserves the right to request that, on the termination of their employment, employees delete the relevant contacts, accounts and information from any social networking site including LinkedIn which they may have linked in with during the course of their employment.

Business Use and Recruitment

Any specific business functions and employees within the Company who as part of their duties are expected or encouraged to use social media for marketing, recruitment or other purposes will be provided with access to specific websites on Company communication

systems. If you require access to such websites during working hours in order to perform and undertake your duties effectively, you should speak to your line manager.

If you are approached by any other employee, client, supplier or any other third party for comments about the Company for publication on any social networking website or blog, you must forward this request immediately to your line manager and should not respond to the request without written approval from your line manager. The Company may require you to undergo training before access is given or impose certain requirements and restrictions on your activities.

The Participation People does not usually permit the use of internet searches on candidates on social networking websites for recruitment and selection purposes. However, internet searches may be used to perform due diligence on candidates in the course of recruitment. On occasions that these searches are used, the Company will act in accordance with data protection and equal opportunities obligations and policies, including the relevant job applicant privacy notice.

Security

Employees must be on guard for social engineering and phishing attempts where scammers may attempt to use deception to obtain information relating to the Company, its management team, clients, business partners or other third parties. Care must be taken not to fall victim to social media scams and employees should never reveal sensitive details (e.g. passwords or client account information) to anyone, including anyone purporting to be part of the Company or acting on its behalf. In this event, the request should be verified and authorised internally.

Social networks are often used to distribute spam and malware. Employees should therefore avoid clicking links in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages and should always check email domains.

You must also not use any new piece of software, application or service with any Company social media accounts without first receiving written approval by your line manager.