Social Media Policy and Procedure

Purpose

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner. This policy sets out the Company's position on use of these on Company media and in work time or your own private media in your own time.

Your responsibilities

Social networking sites and blogs offer a useful means of keeping in touch with friends and colleagues, and they can be used to exchange views and thoughts on shared interests, both personal and work-related. The Company does not object to you setting up personal accounts on social networking sites or blogs on the internet, in your own time and using your own computer systems. However, you must not do so on Company media or in work time.

You must not link your personal social networking accounts or blogs to the Company's website. Any such links require the Company's prior consent. You must not disclose Interr's or our Client's secrets, information's procedures, details, names, breach copyright, defame the Company or its clients, suppliers, customers or any individual who works for the Company, or disclose personal data or information about any individual who works for the Company, colleague, or worker on your blog or on your social networking site.

Social networking site posts or blogs should not be insulting or abusive to employees, workers, contractors, suppliers, Company contacts, clients or customers. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.

Compliance with related policies

Social media should never be used in a way that breaches any of the Company's other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum.

For example, you are prohibited from using social media to:

- breach any of our Information Security policies, incl but not limited to Electronic and Endpoint Device policy and procedure, Mobile Phone policy, Teleworkign, telecommuting and remote working policy, etc..
- breach our obligations with respect to the rules of relevant regulatory bodies
- breach any obligations contained in those policies relating to confidentiality
- breach our Disciplinary Policy or procedures
- harass or bully other staff in any way or breach our Anti-harassment and Bullying Policy
- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities Policy
- breach our Data Protection Policy (for example, never disclose personal information about a colleague online); or
- breach any other laws or regulatory requirements.

You should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the Company.

References to the Company

If reference is made to your employment or to the Company, you should not be making any statements but refer them to your line manager or the Human Resources department. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorised Interr spokespersons. If employees publish content after-hours that involves work or subjects associated with Interr, a disclaimer should be used, such as this: 'The views expressed on this website/blog are mine alone and do not reflect the views of my employer'.

You should always be conscious of your duty to act in good faith and in the best interests of the Company under UK law. The Company will not tolerate criticisms posted in messages in the public domain or on blogs about the Company or any other person, sites or clients connected to the Company. You must not bring the Company or its clients into disrepute through the content of your website entries or your blogs.

Any misuse of social networking sites or blogs as mentioned above may be regarded as a disciplinary offence and may result in dismissal without notice. You should be aware that any information contained in social networking sites may be used in evidence, if relevant, to any disciplinary proceedings.

Business Use of Social Media

If your job duties require you to speak on behalf of the Company in an online social media environment, you must still seek a written approval for such communication from your manager, who may require you to have training before you are permitted to participate in social media on behalf of the Company.

Similarly, if you are invited to comment about the Company for publication anywhere, including in any social media outlet, you should inform your manager and you must not respond without prior written approval from the CEO.

Third parties

You must not disclose any information that is confidential or proprietary to the Company or to any third party that has disclosed information to the Company. This policy should be read in conjunction with the Company's policies on Computers and Electronic Communications and Monitoring and Information Security.

Confidential Information and Intellectual Property

You must not post comments about sensitive business-related topics, such as the Company's or our Client's performance, or do anything to jeopardise trade secrets, confidential information and intellectual property. You must not include the Company's or our Client's branding, logos or other trademarks in any social media posting or in your profile on any social media platform.

Details of business contacts made during the course of your employment are regarded as Company confidential information, and are the property of the Company for a minimum of three years post the terminatin of your employmnet. This includes information contained in databases such as address lists contained in Outlook, or business and contacts lists created and held on any electronic or social media format, including but not limited to LinkedIn and Facebook.

Updating your LinkedIn profile to refer to your new employer and setting up your account to ensure that your contacts receive notification of this will be regarded as an act of unlawful solicitation and/or an unlawful attempt to deal with customers, colleagues, and business contacts of the Company and may result in civil proceedings being brought against you.

Monitoring

The Company reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

Procedure

The following principles apply to professional use of social media on behalf of Interr Security as well as personal use of social media when referencing Interr Security.

- Employees need to know and adhere to the Interr Security's Code of Conduct, Employee Handbook, and other company policies] when using social media in reference to Interr Security.
- Employees should pay particular attention to Interr's Information Security when using social media
- Employees should be aware of the effect their actions may have on their images, as well as Interr Security's image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that Interr Security may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Interr Security, its employees, or customers.

- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.
- Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor/ Line Manager.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized Interr Security spokespersons.
- If employees find encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at Interr Security. Interr Security's computer systems are to be used for business purposes only. When using Interr Security's computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Interr Security blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
- Subject to applicable law, after-hours online activity that violates the Company's Code of Conduct or any other company policy may subject an employee to disciplinary action or termination.
- If employees publish content after-hours that involves work or subjects associated with Interr Security, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent Interr Security's positions, strategies or opinions."; 'The views expressed on this website/blog are mine alone and do not reflect the views of my employer'.
- It is highly recommended that employees keep Interr Security related social media accounts separate from personal accounts, if practical.

Breaches of this policy will be dealt with under the Company's Disciplinary Procedure. You should be aware that the Company regards breach of any part of this policy as gross misconduct that may result in disciplinary action up to and including dismissal without notice.
If you become aware of information relating to the Company posted on the internet, you should bring this to the attention of your manager.

Policy Review and Assessment

This policy may be amended by Interr at any time to take into account changes in legislation and best practice. This policy was last reviewed and agreed by the Board and seeks to be reviewed and updated annually. Any queries arising regarding this policy should be addressed to Mick Tabori.

Mick Tabori - CEO
January 2024