



## **SOCIAL MEDIA POLICY**

### **GENERAL**

This policy document has been produced to provide all SB Security Solutions employees with simple guidelines on how to conduct yourself, have fun and stay safe when using social media.

The use of social media platforms and devices is changing the way we work, interact and socialise. We all have access to, and use, social platforms. The World Wide Web has made all of us potential publishers. SB Security Solutions wants to ensure our staff utilise the social web in an effective and supportive way. This gives our customers, colleagues and any external viewers the best possible understanding of who we are and what we do. It's a great way to engage and communicate, but there are also potential risks that we must all be aware of.

### **PRIVACY SETTINGS**

We appreciate that not all of your social media use will be work related, but you should be aware of what content is visible on your network and who else might be able to view it. Ensure you understand your privacy settings; and use them.

Only allow access to those you really wish to share information with. Remember, what you share with friends "on-line" may also be shared by them; and what you send can quickly become out of control or taken in the wrong context. Do not upload pictures of colleagues unless you have their permission to do so. Be careful, when communicating with non-SB people, about what information you give regarding your work as it may compromise your safety or the safety of a colleague or the business.

### **STAYING SAFE**

Working in the security industry means that we may be targeted by criminals. Do not put yourself, your colleagues or your family at risk. Remember; information about your work, your workplace or your home may be accessed and used by criminals to target you.

Always think carefully about what you put "on-line", and never talk about security processes, locations, procedures or security equipment. Be careful, when posting photographs that identify you or your colleagues in your workplace or in uniform. Also be aware, that if using geo-location media, this will provide information that may target you for attack!

### **STAY LEGAL**

Be careful that what you post does not break the law, any conditions in your Contract, or the Staff Handbook. You must also remain aware that your signed contract contains a Confidentiality clause, which prohibits you from disclosing any confidential information regarding the company or any of our client's information.

When using any company equipment or media platforms, you are also bound by the **IT Communications and Monitoring Policy (QD.12)** which may be viewed, with this policy, on the Staff Portal at any time. Employees can be disciplined by the company for commentary, content, or images that are defamatory, pornographic, harassing or libelous and that can create a hostile work environment or may bring the company into disrepute.

There are new UK GDPR regulations (implemented in January 2018); which relate to "Personal information and Data". You must read and comply with the requirements of the company Policy documentation: **QD.14 GDPR Statement & Privacy Policy**.

You should also be aware that you could be sued by colleagues, competitors, and any individual or company that views your commentary, content, or images as defamatory, pornographic, harassing, libelous or creating a hostile work environment. If in doubt, check. If you are not sure about whether information has been released publicly or doubts of any kind, speak with your line manager or Head Office before releasing information that could potentially harm our company, or our current and potential employees, partners or customers.

## **MANAGE YOUR REPUTATION**

Build your own reputation. Be yourself. Care about what you are talking about. Add value to the conversation. Write what you know. Stick to your area of expertise & provide unique, individual perspectives on what is going on at the company & in your part of the world.

Google yourself. If you want to engage in social media or have done for some time it is always worth seeing what information, images & content is on the web that refers direct to you. Don't spam - Ever. Do feel free to link to other blogs and posts by both company employees and others but do not do it simply to spam the company name to others.

Be a good conversationalist. Monitor and reply to comments in a timely manner, make sure you review comments to tweets and posts etc regularly, you have an audience, don't alienate it. If you are having an emotional response to something, take a break (it is often better to respond the next day) and make sure your response is appropriate – or show someone else first before you send it. Ensure that all images you use are shareable so that others can pass on your work to other interested parties.

## **PERSONAL & WORK ISSUES**

Social networks blur the lines between public and private, personal and professional. Just by identifying yourself as a SB Security Solutions employee, you are creating perceptions about your expertise and that of the company. You can express your own opinion, but please make it clear the opinion is yours & not the companies. Similarly, the company logo & trademarks may not be used without explicit permission in writing from the company.

Remember, while media sites are an excellent way to share thoughts, there are other, more appropriate channels, to use; particularly if you are not happy with something, especially at work. If you have an issue with a colleague, manager or something that the company has done, there are internal channels that you should use, including your line manager and the HR department.

## **ON-LINE ISSUES**

Share! The company values Teamwork and Collaboration & we believe in sharing & linking to the best content from all over the web. A link is not an endorsement, so do not be shy about sharing something from another source if you feel it is worthwhile.

Speak up on positive news. If you see something posted that you like, say so. Mention it to others or link to it. Tell others about it. Also speak up when you disagree. If you see something posted that you feel is derogatory, offensive or incorrect, respond or flag it up to your line manager or speak with Head Office.

Social media is a great opportunity to show that we understand and acknowledge issues and deal with them appropriately – both as a company and as individuals. Avoid confrontation: others are also entitled to air their opinion, even if it does not match your own.

## **MISTAKES**

Sometimes mistakes happen...

If you are concerned that you have made a mistake or error of judgment, then let your line manager or Head Office know as soon as possible. Don't ignore mistakes – the sooner an issue is addressed, the more likely the impact will be reduced and together we can agree the best course of action. Please observe these simple but effective guidelines on how to conduct yourself, have fun and stay safe when using social media.

This policy document shall be made available to all employees, at induction and via the staff portal web site, at; [www.sbsecuritysolutions.co.uk](http://www.sbsecuritysolutions.co.uk). **This policy shall be reviewed annually or if legislation, regulations or company policy changes dictate.**

*S Bettsworth*

**Steve Bettsworth  
Managing Director**

*S Bettsworth*

**Sharon Bettsworth  
Media Representative**