SOCIAL MEDIA POLICY

DOCUMENT CONTROL:

- Policy Reference: GF06
- Version Number: 03
- Author: Jess Cantrill
- Date of Last Review: Aug 2022
- Date of Next Review: Aug 2023

REVISION HISTORY:

Version Number	Version Date	Nature of Change	Date Approved
01	Sep 2019	Policy re-written	Sep 2019
02	May 2022	Policy rebranded & updated in line with current BCP.	May 2022
03	Aug 2022	Amended & further approved.	Aug 2022

CONTENTS:

1. POLICY STATEMENT

1.1. Your use (personal or business) of social media can pose risks to our confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

1.2. To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes, you must adhere to this policy.

1.3. This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. WHO IS COVERED BY THE POLICY?

2.1. This policy covers all individuals working at all levels, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff, and volunteers (collectively referred to as 'staff' or 'you' in this policy).

2.2. Third parties who work with us and/or have access to our electronic communication systems and equipment are also required to comply with this policy.

3. THE SCOPE AND PURPOSE OF THE POLICY

3.1. This policy applies to the use of all forms of social media, including Facebook, TikTok, LinkedIn, Twitter, Google+, Wikipedia, Whisper, Instagram, Vine, Tumblr, personal WhatsApp accounts and all other social networking sites, internet postings, messages, apps and blogs.

3.2. There are many ways to access social media, through apps, internet sites, blogs, etc. and this policy applies to any form of connection to social media, regardless of ownership of the account or equipment.

3.3. This policy applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or your own equipment.

3.4. Social media is but not limited to, a broad category or genre of communications media which occasion or enable social interaction among groups of people, whether they are known to each other or strangers, localised in the same place of geographically dispersed. It includes new media such as newsgroups, MMOGs, and social networking sites. Such media can be thought of metaphorically as virtual meeting places which function to occasion the exchange of media content among users who are both producers and consumers. Social media has also become adopted as a significant marketing tool. More than 4.5 billion people use social media as of June 2022.

4. PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF THE POLICY

4.1. All managers have a specific responsibility to operate within the boundaries of this policy, ensure that all staff understand the standards of behaviour expected of them, and to take action when behaviour falls below its requirements.

4.2. You are responsible for supporting colleagues and ensuring the success of this policy. Staff should ensure that they take the time to read and understand it. If you are unsure about

any of the content or the application of this policy, it is your responsibility to speak to your manager.

4.3. If you become aware of any misuse of social media, you should report it to your manager or a member of senior management.

5. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

5.1. Social media (personal or business use) should never be used in a way that breaches any of our 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:

5.1.1. breach the company IT and Communications Systems policy;

5.1.2. breach the company obligations with respect to the current applicable local laws, rules and regulations of any relevant regulatory bodies;

5.1.3. breach any obligations relating to confidentiality or intellectual property; unless otherwise stated the company will own any and all intellectual property created by a user of the company networks.

5.1.4. breach the company disciplinary rules or procedures;

5.1.5. defame or disparage the organisation or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders;

5.1.6. harass or bully other staff in any way (including in breach of our Anti-harassment and Bullying Policy);

5.1.7. unlawfully discriminate against other staff or third parties (including in breach of our Equal Opportunities Policy);

5.1.8. breach our Data Protection Policy (for example, never disclose personal information about a colleague online); exclusions to this clause include disclosure to local authorities, payroll information to the payroll bureau, care must be taken to ensure only relevant data is transmitted in any circumstance.

5.1.9. breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as claiming to be someone other than yourself or by making misleading statements). You should also be aware of our Anti-Corruption and Bribery Policy.

5.2. You should never provide references or recommendations 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 organisation without senior manager approval. Any requests for individuals references must be referred to HR in the first instance. Credit reference requests must be referred to finance.

6. PERSONAL USE OF SOCIAL MEDIA AT WORK

6.1. You may use your own devices to access social media during your designated break times so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity, and complies with this policy. Personal use of social media (even using your own devices) is not permitted during working time.

6.2. You must never access the following for personal use from our network or equipment or devices (including smartphones or tablets given to you for business use): online radio, audio and video streaming, instant messaging, webmail (such as Gmail or Hotmail) and social networking sites (including, but not limited to, Facebook, Twitter, TikTok, YouTube, Google+, Instagram, SnapChat, Pinterest, Tumblr, Second Life, personal WhatsApp accounts). This list is not exhaustive and remains subject to change at the company's discretion.

7. RESPONSIBLE USE OF PERSONAL SOCIAL MEDIA ACCOUNTS

7.1. Following this policy will ensure you are using social media responsibly and safely.

7.2. You are personally responsible for what you communicate in social media whether using our equipment or not and whether posting in your own time or not. Remember that what you publish might be accessible to be read by the masses (including the company, future prospective employers and social acquaintances). Keep this in mind before you post content.

7.3. You may believe that your posts on social media are private or can only be viewed by a few, but often even the most secure privacy settings cannot prevent your friends, connections or contacts from passing them on and bringing them into public view.

7.4. Whilst your personal profiles are your own, what you post and how you manage your accounts (whether using our equipment and systems or not and whether in your own time or not) can impact our reputation and business and your association with us can cause us to be liable to third parties for your action. Failure to use your accounts responsibly may result in disciplinary action. Your attention is drawn to Compliance with Related Policies and Agreements above.

7.5. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your manager.

7.6. You should use your common sense to avoid creating any issues for us as an organisation through your use of social media. The following rules will also assist you:

7.6.1. Unless you have been given clear prior authority to do so, you must not identify; mention; comment on; or refer to any information relating to us; your colleagues or members of staff; our customers or clients; suppliers and vendors; other affiliates and stakeholders; and any other people who could reasonably be associated with us.

7.6.2. You should make it clear in social media postings that you are speaking on your own behalf. Write in the first person and use a personal e-mail address when communicating via social media.

7.6.3. If you disclose your affiliation with us on your profile or any social media postings, you must also state that your views do not represent those of the company. For example, you could state, "the views in this posting do not represent the views of the company or its management". You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

7.7. If you see content in social media that disparages or reflects poorly on us; your colleagues or members of staff; our customers or clients; suppliers and vendors; other affiliates and stakeholders; and any other person who could reasonably be associated with us, you should contact the IT manager. All staff are responsible for protecting the business.

8. BUSINESS USE OF SOCIAL MEDIA

8.1. Blogs and social media can offer exciting and innovative ways for our business to thrive. However, unless this type of marketing or business development is directly part of your role, we do not wish you to participate in them without your manager's approval.

8.2. If you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the inquiry to the IT manager.

8.3. If your duties require you to speak on behalf of the organisation in a social media environment and/or you are associated with us on any professional networking site (including LinkedIn), you must still seek approval for the communications you make from the IT manager who may require you to undergo training on permitted use and impose certain requirements and restrictions with regard to your activities.

8.4. We will usually require you to create business profiles on social media and you are not permitted to use personal accounts for business usage under any circumstances. In the unlikely event of existing personal accounts been utilised for business use, please close these accounts and transfer any and all posts to a bona-fide business account.

8.5. The contact details of business contacts made during the course of your employment (whether on business or personal accounts) are regarded as confidential information belonging to the company and your obligations under your contract of employment will apply. This may include deleting any such confidential information from your accounts (business or personal) at any time including on termination of your contract of employment (by way of dismissal or voluntary notice).

8.6. In addition to complying with our policies and procedures (see Compliance with Related Policies and Agreements above), seeking approval from your manager, and always acting in the best interests of the organisation, the following guidelines must be followed when using social media for business use:

8.6.1. Make sure that your online postings and communications reflect your level of expertise, and that you limit your comments to your area of knowledge.

8.6.2. Try to stimulate interest in the work that you are doing and invite a dialogue so that you can learn from others doing similar or related things.

8.6.3. Consider the value of your contribution before you post. Examples of adding value include: solving a problem, helping others in the online community, or improving the company's' image.

8.6.4. If you post something in error, act immediately to correct it and accept responsibility when required.

8.6.5. Engaging in arguments and inflammatory debates can tarnish your credibility and reputation, and by association the company's reputation. If you choose to disagree with others online, do so respectfully and objectively and qualify that the opinions you are expressing are yours and yours alone and do not necessarily reflect the views of the management of the company.

8.6.6. Never post anything that might be offensive to others, such as sexual comments or racial slurs. Remember that talk of religion, culture or politics can also easily offend others.

8.6.7. Do not use social media in a false or misleading way, for example, by claiming to be someone other than yourself or by creating an artificial "buzz" around our business, products or shares.

8.6.8. Do not cite or refer to our customers, vendors, business associates or investors, identify them by name or reveal any information (confidential or otherwise) related to them without getting their explicit (written) permission in advance. Also, do not discuss or conduct business with a customer, supplier, business associate or investor in an online forum.

8.6.9. Disclosing or commenting on the company's businesses confidential information is absolutely prohibited, whether in relation to sales, customer lists, financials, business or marketing plans, performance or prospects. Do not comment in any way on rumours about these. If asked directly, refer the inquiry to a relevant departmental manager.

8.6.10. Review the terms of use of all social media sites you access (via the internet or otherwise) and ensure you comply with them. If you need any assistance identifying the terms of use, please ask your IT department for clarification.

9. BREACH OF THIS POLICY

9.1. Breach of this policy (regardless of whether it is committed during working hours, using personal or business accounts or using our equipment) may result in disciplinary action up to and including dismissal. If you are suspected of committing a breach of this policy you will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details of accounts used in the course of work, including a professional Twitter or LinkedIn account.

9.2. You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request will result in disciplinary action.

10. MONITORING AND REVIEW

10.1. We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

10.2. We reserve 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.

10.3. For further information, please refer to our Information and Communications Systems Policy.

10.4. Line Managers and team leaders will be responsible for general monitoring of these guidelines in the first instance. Transgressions will be reviewed with individual staff members, but in some cases, it may be appropriate to record examples for discussion as part of staff training or discussion at team meetings.

10.5. Significant and/or repeated breaches of this policy will lead to disciplinary action, up to and including dismissal.

11. RELATED POLICIES

11.1. HR02- Equal Opportunities Policy
11.2. HR19- Anti-corruption & Bribery Policy
11.3. HR20- Anti-harassment & Bullying Policy
11.4. GF02- IT & Communications Systems Policy
11.5. GF03- Data Protection Policy