SecureCare
SOCIAL MEDIA POLICY

SecureCare (the "Company") recognise that the internet provides unique opportunities to participate in interactive discussions and share information on topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. Your use of social media can pose risks to our confidential and proprietary information, and reputation, and can jeopardise our compliance with legal obligations.

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, we expect you to adhere to this policy.

Scope and Purpose of the Policy

This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

It 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 equipment belonging to members of staff.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

You may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

The purpose of this Policy is to minimise the various risks to the Company presented by Social Media usage.

In addition to this Policy, Users must also comply with other Company Policies including the Company's Data Protection Policy, Equal Opportunities and Diversity Policy, and Harassment and Bullying Policy

General Principles

There are certain general principles that all Users should keep in mind when using Social Media, whether for personal use or for authorised work-related purposes. All Users must:

- Use Social Media responsibly and professionally, and at all times in accordance with their duties
- Be mindful of what constitutes confidential, restricted, or other proprietary information and ensure that such information is never disseminated over Social Media without express authority
- Be mindful of what constitutes personal data and ensure that personal data relating to staff and customers is never disseminated over Social Media unless it is used in accordance with the Company's Data Protection Policy and with express authority
- Ensure that their use of Social Media does not breach any other of the Company's policies including, but not limited to, its Data Protection Policy, Equal Opportunities and Diversity Policy, and Harassment and Bullying Policy
- Ensure that their use of Social Media does not breach any other laws, regulatory requirements, or other applicable rules set out by regulatory bodies and other organisations
- Ensure that they do not breach any copyright or other intellectual property rights when using Social Media

- Be mindful of the fact that any communication may be relied upon in court, to the advantage or detriment of the individual or the Company and conduct their use of Social Media accordingly

The viewing, transmission, downloading, uploading, or accessing in any way, whether through Social Media or otherwise, of any of the following material using the Company's Internet and Communication Facilities will amount to gross misconduct with the possibility of summary dismissal:

- Material which is pornographic, sexist, racist, homophobic, or any other discriminatory or otherwise obscene or offensive material
- Illegal or criminal material, including material which breaches copyright or any other intellectual property right
- Any material which has the object or effect of causing harassment to the recipient
- Material which the User knows, or reasonably ought to know, is confidential, restricted, or otherwise proprietary information and which they are not authorised to deal with
- Any website (Social Media or otherwise) which the Company has blocked access to

Personal Social Media Use

Users may use Social Media for personal purposes occasionally during work hours for example, during breaks provided that such usage complies with the provisions of this Policy and provided that it does not interfere with their work responsibilities or productivity.

Business Social Media Use

Certain Users may from time to time be required to use Social Media on behalf of the Company. Users should only do so with the authorisation of their line manager, in accordance with instructions issued by the Managing Director, and in accordance with this Policy.

Use of Social Media for business purposes must comply with the provisions of this Policy at all times.

Users using Social Media on behalf of the Company may from time to time be required to interact with other internet users via Social Media, for example, in response to posts or enquiries regarding the Company. Unless the instructions issued to that User specifically authorise the User to respond without further approval, the User may not respond to any such communications without the prior approval of the Directors.

In any event, no User using Social Media on behalf of the Company should respond to such communications, with or without prior approval, without first consulting the relevant individual and/or department unless they are fully knowledgeable of the relevant topic and suitably qualified to respond.

Social Media contacts made during the course of business are to be treated as confidential information belonging to the Company.

Before using Social Media on behalf of the Company, Users may require training in order to do so, or may be required to demonstrate that they have already received suitable training, either from the Company or from a previous employer or other organisation.

Acceptable Use of Social Media

If a User makes any posting, contribution, or creation or publishes any other content which identifies or could identify the User as an employee, contractor, agent, or other member or associate of the Company, or in which the User discusses their work or experiences relating to the Company, the User must at all times ensure that their

conduct is appropriate and consistent with their contract of employment and the corporate image of the Company, and should bear in mind that the User owes a duty of fidelity to the Company.

Unless specifically instructed to do so by the Directors, Users should make it clear that they are posting on Social Media as themselves, not as the Company, and that all opinions and ideas expressed on Social Media by that User are those of the User and do not necessarily reflect the views of the Company.

Unless using Social Media on behalf of the Company, Users should not use any Social Media accounts belonging to (or otherwise associated with) the Company.

Company email addresses may not be used to sign up to any Social Media websites.

Users should always be respectful to others when using Social Media and should always be mindful of the fact that their association with the Company may be known to anyone at any time. The conduct of all Users on Social Media may reflect on the Company, whether positive or negative. This applies whether a User is using Social Media for business purposes or for personal purposes, whether during workings hours or otherwise.

If a User is unsure as to the appropriateness of a posting or other content they wish to publish, they should speak to Robert Stevenson at the earliest opportunity to seek clarification.

Unacceptable and Prohibited Use of Social Media

Users must refrain from doing anything on Social Media or any other websites that defames, disparages, or otherwise brings into disrepute, the Company, a User's superiors, a User's colleagues, or other related third parties. This includes, but is not limited to, making false or misleading statements and impersonating colleagues or third parties.

Users must ensure that their use of Social Media does not damage the Company, its interests, or its reputation, whether directly or indirectly, in any way.

Unless specifically instructed to do so, Users must not represent themselves on Social Media as the Company or as posting on behalf of the Company.

Users may not share the following on Social Media unless specifically authorised to do so by the Directors:

- Confidential information
- Commercially sensitive or other proprietary business information belonging to or about the Company or any of its employees, contractors, agents, or other affiliated third parties and organisations
- Personal data relating to individuals, staff or customers

Users may not use any intellectual property belonging to the Company on Social Media (including, but not limited to, trade marks and logos) unless specifically authorised to do so by the Directors.

Users may not add contacts made during the course of their duties to their personal Social Media accounts without the authorisation of the Directors and without the express consent of the individuals involved.

Monitoring

To the extent permitted or required by law, the Company may monitor Users' use of the Company's Internet and Communications Facilities (including, but not limited to, Social Media use) for its legitimate business purposes which include (but are not necessarily limited to):

- Ensuring that Company policies and guidelines are followed, and standards of service are maintained

- Complying with any legal obligation
- Investigating and preventing the unauthorised use of the Company's Internet and Communications Facilities and maintaining security
- Investigating the suspected viewing or sending by Users of offensive or illegal material (or material that is otherwise in violation of this Policy)
- Investigating a User suspected of spending an excessive amount of time using the Company's Internet and Communications Facilities for personal purposes

Users should be aware that all internet traffic data sent and received using the Company's Internet and Communications Facilities (including, but not limited to Social Media use) is logged, including websites visited, times of visits, and duration of visits. Any personal use of the internet will necessarily therefore be logged also.

Users who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations.

By using the Company's Internet and Communications Facilities for personal use, Users are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of Users' use of the Company's Internet and Communications Facilities complies with all relevant legislation including, but not limited to, the GDPR (EU Regulation 2016/679 General Data Protection Regulation) and the Human Rights Act 1998.

Recruitment

The Company may use internet searches to carry out due diligence as part of its recruitment process. In these circumstances, the Company will act in accordance with its equal opportunities and data protection obligations.

Misuse and Compliance

Any User found to be misusing the Company's Internet and Communications Facilities (including, but not limited to, Social Media use) will be treated in line with the Company's Disciplinary Policy and Procedure. Misuse of the internet can, in some cases, amount to a criminal offence.

Where any evidence of misuse of the Company's Internet and Communications Facilities (including, but not limited to Social Media use) is found, the Company may undertake an investigation into the misuse in accordance with the Company's Disciplinary Policy and Procedure. If criminal activity is suspected or found, the Company may hand over relevant information to the police in connection with a criminal investigation.

This Policy will be regularly reviewed and updated as necessary. The management team endorses these Policies and is fully committed to their implementation.

This Social Media Policy has been approved & authorised by:

Signature:

Signed by: ROBERT STEVENSON
Position: DIRECTOR

Date:
Review date: