**Use of Email, Internet, and Telecommunication**

Email enables us to communicate promptly and efficiently with our customers and suppliers. While email brings many benefits to us in terms of its communications, it also brings risks to us. For this reason, we must lay down specific rules for using email and the Internet within our business.

You are responsible for maintaining our image, using electronic resources productively and avoiding placing us at risk of legal or commercial liability based on your use. You must ensure that current General Data Protection Regulation (GDPR) legislation is not breached, and where a breach occurs, that you report it without delay to the person responsible for general data protection within the business/Company.

You are not allowed to use email for private purposes and should not use it for any purpose other than Company business.

We may have Internet access to enable you to obtain information specific to your role. If you require access to the Internet in connection with your part, you will need the approval of your line manager and any such Internet connection is intended to support Company business. Internet use for private purposes is prohibited without the specific prior consent of your line manager and senior management.

You must not disclose any inappropriate and confidential information regarding us using the Internet (including via any social media platform), email or other means.

You may only download material which is required for our business purposes.

All software is our property and should not be misused or copied. You must comply with all protocols and directives regarding Internet security.

The above applies equally to other equipment and technology, such as telephones, fax machines and other communication devices.

We reserve the right to monitor all your use of emails, the Internet, software, and technological equipment. You should have no expectation of privacy regarding your use of these facilities.

**Definition of Social Media**

For this policy, social media is any online platform or app allowing parties to communicate instantly or share data publicly. This includes social outlets such as Twitter, Facebook, and LinkedIn. Social media also covers blogs and video and image-sharing websites such as YouTube.

You should be aware that there are many more examples of social media than can be listed here, and this is a constantly changing area. You should follow these guidelines concerning any social media you use.

[Delete Option 1 or Option 2 as appropriate]

**Use of Social Media at Work**

OPTION 1 (strict ban on the use of social media at work)

You cannot access social media from our computers or devices anytime. This includes computers or devices distributed by us for work purposes.

[We have specifically blocked the use of [Twitter/Facebook/other social media websites blocked] on its computers.]

We understand you may wish to use your computers or devices to access social media at work. You must limit your use of social media on your equipment to your official rest breaks, such as your lunch break/times when you are unemployed/appointments, for example, travelling times/times when you are not on duty.

OPTION 2 (open use of social media at work)

We encourage you to make reasonable and appropriate use of social media websites for your work. It is an important part of how we promote our services and communicate with our audience as it allows communication between its employees.

[However, your Employer has specifically blocked the use of [Twitter/Facebook/other social media blocked] on its computers.]

We understand that you may use your own computers or devices to access social media while at work. You must limit your use of social media on your own equipment to your official rest breaks, such as your lunch break/times when you are unemployed/appointments, for example, travelling time/times when you are not on duty.

You can contribute to our social media activities by writing our blogs/managing our Facebook account/running an official Twitter account for us.

You must always know that you represent us while contributing to our social media activities. Staff who use social media as part of their job must adhere to the following rules.

You should use the same safeguards as any other form of communication about your Employer in the public sphere. These safeguards include:

• Make sure that the communication has a purpose and a benefit for your Employer;

•obtaining permission from a manager before embarking on a public campaign using social media; and

•getting a colleague to check the content before it is published.

**Excessive Use of Social Media at Work**

It would be best not to spend excessive time engaged in personal social media while at work. This is likely to have a detrimental effect on your productivity. You should ensure that social media does not interfere with your other duties.

**Monitoring Use of Social Media During Work Time**

We reserve the right to monitor your use of social media on our equipment. We will consider that valid reasons for checking an employee's internet usage include suspicions that you have been using social media when they should be working; or acted in a way that is in breach of the rules set out in this policy.

Monitoring will be conducted in accordance with an impact assessment that the organisation has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the organisation's legitimate interests and ensures that this policy on the use of social media is being complied with.

The data controller is as per the Data Protection Policy. Monitoring will consist of checking the social media sites that have been visited, the duration of such visits and the content you have contributed to such sites.

Monitoring will normally be conducted by our [Employer's security team.]The information obtained through monitoring may be shared internally, including with HR team members, your line manager, managers in the business area where you work, and IT staff if access to the data is necessary to perform their roles. However, information is usually shared in this way only if we have reasonable grounds to believe there has been a breach of the rules in this policy.

Information obtained through monitoring will not be disclosed to third parties (unless we have a duty to report matters to a regulatory authority or a law enforcement agency).

Workers have several rights about their data, including the right to make a subject access request and to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in your Employer's data protection policy. You can complain to the Information Commissioner if we do not comply with your data protection rights.

Access to particular social media may be withdrawn in any case of misuse.

**Social Media in Your Personal Life**

We recognise that you make use of social media in a personal capacity. While you are not acting on behalf of ourselves, you must be aware that you can damage us if you are recognised as one of our employees.

You can say that you work for us, and we recognise that it is natural for you sometimes to want to discuss your work on social media. However, your online profile (for example, the name of a blog or a Twitter name) must not contain our name.

Suppose you discuss your work on social media (for example, giving opinions on your specialism or the sector in which we operate). In that case, you must include a statement along the following lines on your profile: "The views I express here are mine alone and do not necessarily reflect the views of my employer."

Any communications you make in a personal capacity through social media must not:

Bring us into disrepute, for example, by:

criticising or arguing with customers, other employees, or rivals;

making defamatory comments about individuals or ourselves or groups; or

posting images that are inappropriate or links to inappropriate content;

Breach confidentiality, for example, by:

revealing trade secrets or information owned by ourselves

giving away confidential information about an individual (such as another employee’s or customer’s contact information) or another Employer (such as a rival business); or

discussing our internal workings (such as deals that it is doing with a customer/client or its future business plans that have not been communicated to the public);

Breach copyright, for example, by:

using someone else's images or written content without permission;

failing to give acknowledgement where consent has been shown to reproduce something; or

Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example, by:

making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;

using social media to bully another individual (such as an employee of your Employer); or

posting images that are discriminatory or offensive or links to such content.

**Use of Social Media in the Recruitment Process**

Unless it is about finding candidates (for example, if an individual has put their details on social media websites to attract prospective employers), the HR department and managers should not, either themselves or through a third party, conduct searches on applicants on social media.

However, we may conduct social media searches on applicants when their social media activity is directly relevant to their skills or claims made in the recruitment process. For instance:

a candidate might claim that they have used social media in their previous job (for example, as a publicity tool); or

a candidate’s social media use may be directly relevant to a claim made in their application (for example, if they run a blog based around a hobby mentioned in their CV or a skill they claim to be proficient in).

There should be no systematic or routine checking of a candidate’s online social media activities. This is because conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with your Employer's equal opportunities policy.

**Resolution Action Over Social Media Use**

You are required to adhere to this policy. You should note that any breaches of this policy may lead to resolution action. Serious breaches of this policy, for example, incidents of bullying of colleagues or social media activity that might cause serious damage to ourselves, may constitute gross misconduct and lead to summary dismissal.