SOCIAL MEDIA POLICY

The Red Industries Group recognises that social interaction on the internet is an important and integral part of life. Social media should be used correctly, where there is no detrimental impact to yourself or against the business, whether this is inside or outside of working hours.

Guiding Principles
Social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes social forums such as Twitter, Facebook, Snapchat, Instagram, Tik Tok, Whatsapp and LinkedIn. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr.

Employees should be aware that there are many more examples of social media and communication platforms than can be listed here and this is a constantly changing area.

Where the policy refers to social media this encompasses all social media forums and communication platforms available.

Any use of social media, inside or outside of working hours should not expose you or Red to legal liability.

This policy should be read alongside other key policies. The company's IT & Equipment Policy, Communications Policy and Data Protection Policy are particularly relevant to employees using social media.

Use of Social Media – Personal
Employees are allowed to access social media websites from the organisation's computers or devices at certain times.

The organisation understands that employees may also wish to use their own computers or devices, such as laptops and hand-held devices, to access social media websites while they are at work.

Employees must limit their use of social media to their official rest breaks such as their lunch break or at times when they are between jobs or appointments, for example travelling.

Employees should ensure their use of social media does not interfere with their other duties as it is likely to have a detrimental effect on employees' productivity.

If using social media is part of your role, your line manager will discuss how much time should be dedicated to it.

Employees should make it clear that you are speaking in your personal capacity and not as a Red representative.

If you choose to include contact information this should be your personal details and not work contact details.

If you elect to disclose your connection to Red, then you must clearly and expressly state that your views do not represent those of the Employer.

A misjudged status update can generate complaints or damage the company's reputation. There are also security and data protection issues to consider.

Unless the social media account and/or conversation platforms are being used for business purposes, employees should not sign up to social media platforms and/or conversation platforms using their Company email address or Company mobile phone number.

Last revised: 13.06.22

Use of Social Media – Official Enquiries
Any media enquiries via social media should be directed to the Group Marketing Manager. If you are contacted by a media representative or asked for comment for publication about us or otherwise in connection with your employment, you should inform the Group Marketing Manager. You would not be authorised to respond the enquiry on behalf of the company.

Use of Social Media – Business
For some roles within the organisation, the use of social media websites is part of their work. Roles in Sales, Marketing and Human Resources departments will be encouraged to make appropriate use of social media websites as part of their day-to-day job.

Employees will be encouraged to promote recruitment vacancies, sales offers or information on our products.

Any social media accounts and/or conversation platforms linked to an employees Company email address and/or Company mobile number will need to be closed down at the point of the employee leaving the business.

Whilst interacting on social media employees should use the same safeguards as they would with any other form of communication about the organisation in the public sphere. These safeguards include:

- making sure that the communication has a *purpose* and a *benefit* for the organisation;
- getting a colleague to *check the content* before it is published.

Guidance on Social Media Use
Any communications that employees through social media must not:
- ***bring the organisation into disrepute,*** for example by: criticising or arguing with customers, colleagues or rivals; making defamatory comments about individuals or other organisations 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 the organisation; giving away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a rival business); or discussing the organisation's internal workings (such as deals that it is doing with a customer 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 permission has been given to reproduce something;
- ***breach intellectual property rights,*** for example by: not appropriately referencing sources or citations correctly.
- ***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 the organisation); or posting images that are discriminatory or offensive or links to such content.
- ***Create misunderstandings,*** for example by: commenting on sensitive topics or making innocent comments that could be misconstrued. Tone and language of comments can be easily misinterpreted.

Copyright
Red Industries respects and operates within copyright laws. Employees may not use social media to:
Publish or share any **copyrighted software, media or materials owned by third parties**, unless permitted by that third party.

If employees wish to **share content published on another website**, they are free to do so if that website has obvious sharing buttons or functions on it.

Share links to **illegal copies** of music, films, games or other software.

Company social media accounts should be **protected by strong passwords** that are changed regularly and shared only with authorised users.

Last revised: 13.06.22

Wherever possible, employees should use **two-factor authentication** (often called mobile phone verification) to safeguard company accounts.

Avoid Social Scams
Employees should watch for **phishing attempts**, where scammers may attempt to use deception to obtain information relating to either the company or its customers.

Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.

Employees should **avoid clicking links** in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague sounding direct messages.

Following these simple rules helps avoid the most common pitfalls:
Know the social network. Employees should spend time becoming familiar with the social network before contributing. It's important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.

If unsure, don't post it. Employees should err on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or offence — or be otherwise unsuitable — they should not post it. Employees can always consult the Group IT Manager for advice.

Be thoughtful and polite. Many social media users have got into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.

Look out for security threats. Employees should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware.

Keep personal use reasonable. Although the company believes that having employees who are active on social media can be valuable both to those employees and to the business, everyone should exercise restraint in how much personal use of social media they make during working hours.

Don't make promises without checking. Some social networks are very public, so employees should not make any commitments or promises on behalf of Red Industries without checking that the company can deliver on the promises.

Handle complex queries via other channels. Social networks should not resolve complicated enquiries and customer issues. Once a customer has made contact, employees should handle further communications via a more appropriate channel — usually email or telephone.

Don't escalate things. It's easy to post a quick response to a contentious status update and then regret it. Employees should always take the time to think before responding and hold back if they are in any doubt at all.

It is useful to bear in mind when posting any content or comment that they may be permanently and publicly available and that you may not be able later to delete or remove them.

You should ensure that your communications are consistent with the image that you would like to present publicly including to us and any future employers, colleagues, friends, business contacts.

Monitoring use of social media during work time
The organisation reserves the right to monitor employees' internet usage but will endeavour to inform an affected employee when this is to happen and the reasons for it. The organisation considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been spending an excessive amount of time using social media websites for non-work-related activity; or
- acted in a way that is in breach of the rules set out in this policy.

Monitoring will normally be carried out by our IT systems provider.

Personal information obtained through monitoring may be shared internally, including with members of the HR team, your line manager, managers in the business area in which you work and member of the IT team if access to the information is necessary for performance of their roles. Information is only shared internally if we have reasonable grounds to believe that there has been a breach of this policy. We will not share information gathered from monitoring with third parties, unless we have a duty to report matters to a regulatory authority or law enforcement agency.

Access to any Company Social Media accounts can be withdrawn at any point if there is evidence of misuse.

Disciplinary action over social media use
All employees are required to adhere to this policy.

Employees should note that any breaches of this policy may lead to disciplinary action.

Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

Miscellaneous
This procedure will be periodically reviewed. Any amendment to it will be notified to employees in writing by the organisation's Group HR Manager and such written advice will inform employees as to the date when any amendment comes into effect.

I have read and understand the Social Media Policy.

Print Name

Signature

Date