Social Media Policy

This policy applies to all companies within the Relyon Group.

This policy is in place to promote responsible usage of social media whilst minimising the risks to our business through inappropriate use of social media and to ensure staff understand their obligations with regard to the use of social media.

This policy deals with the use of all forms of social media, such as Facebook, LinkedIn, Twitter, Wikipedia, Whisper, Instagram, WhatsApp, Tik Tok, YouTube and all other social networking sites, internet postings and blogs.

It applies to the use of social media for business purposes as well as personal use that may affect our business in any way.

This policy does not form part of any employee's contract of employment and may be amended at any time and any changes will be communicated to staff prior to becoming effective.

Purpose

The purpose of this policy is to inform staff of their obligations with regard to their own use of social media. If any member of staff, when dealing with Relyon customers, is subject to harassment or derogatory comments via social media, they should bring this to the attention of their line manager or a more senior manager as appropriate.

Should anyone within the company come across a derogatory social media post that refers to a Relyon employee by name, they will inform the employee's line manager. The norm would be to discuss the post with the affected employee, however this will be considered on a case by case basis. The post will be reported to the social media platform. The employee's line manager will deal with the customer's complaint following the same procedures for offline communications. It may also be necessary to provide a copy of the post to the Information Security Manager, who will assess if the nature of the content justifies informing the police or other relevant authorities.

Roles & Responsibilities

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the Head of Group Services who will review this policy periodically to ensure that it meets legal requirements, draws upon best practice and reflects developments in social media use and technology.

Managers have responsibilities for the effective implementation of this policy. This includes ensuring that their team members are given the opportunity to read and understand the policy and are aware of the standards of behaviour expected. Managers are not expected to monitor social media use from their team members but are expected to take action when they are made aware of behaviour which falls below the level required.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it, adhere to the requirements described and ensure that their use of social media involving reference to the company does not damage the reputation of the business.

Any misuse of social media should be reported to the relevant member of staff's line manager and in turn to the Head of Group Services. Questions regarding the content or application of this policy should be directed to the Head of Group Services.

Personal Use of Social Media

Unreasonable use of social media for personal matters is not permitted during working hours or by means of ICO computers, devices, networks and other IT resources and communications systems. This could potentially lead to disciplinary action.

It is recognised that you may wish to monitor social media channels for work purposes via a personal account, for example following the Twitter feeds or Linked-in postings of the ICO or relevant stakeholders. This can provide the organisation with useful insight into how we are perceived and how we can develop our services.

Such monitoring must be relevant to your work and must not compromise any investigations or other activities undertaken by the Company. It must not negatively impact on the time you spend on your Social Media core duties or be a mask for personal use of social media in work time. If you become aware of matters which are relevant to the business of Relyon through social media monitoring, you should raise the issue with your Line Manager.

For social media sites or applications which are solely work or professionally based, such as LinkedIn or professional networking forums, you are permitted to state that you work for Relyon, and the capacity of your employment. Before doing so, you should consider if this is relevant or necessary, and if there are any security implications of doing so. For example, if you are involved in high priority investigations it may not be advisable to provide details of your role. Further advice is available from the Head of Group Services or the Security Operations Director. Where your social media accounts are for personal use only, you must not say that you work for Relyon.

Prohibited Use

You must not make any social media communications that could damage our business interests or reputation, whether directly or indirectly.

You must not use social media to:

- Defame or disparage the company, our staff or any third party.
- To harass, bully or unlawfully discriminate against staff or any third parties.
- To make false or misleading statements.
- To directly or indirectly make derogatory comments or use offensive or inappropriate language in any social media communication.
- To impersonate colleagues or third parties.

You must not express opinions or provide advice on behalf of the company via social media, unless expressly authorised to do so by your manager.

You should note that if you provide advice on social media in a personal capacity on matters which relate to the company's responsibilities, it is often easy for you to be identified as connected to the company. Therefore, your advice may be interpreted as reflecting an official Relyon line. You should therefore avoid exposing yourself to a situation where your advice or views could potentially be interpreted as those of the Company. Speak to your manager as soon as possible if you think that there is a risk that this may have occurred.

You must not post comments about sensitive business-related topics, such as our clients, activities or performance, or do anything to jeopardise our investigations, confidential information and intellectual property.

You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

Any misuse of social media should be reported to the relevant member of staff's line manager and in turn to the Head of Group Services and may result in disciplinary action in accordance with the company's disciplinary policy.

Disciplinary sanctions will be as described in the disciplinary policy, up to and including dismissal, depending on the nature of the misconduct identified. Examples of what may be regarded as gross misconduct include (but are not limited to): posting derogatory or offensive comments about Relyon, colleagues, or customers; the deliberate or negligent disclosure of information about the company's activity and the posting of comments which may cause harm to the reputation of the company.

Business Use of Social Media

If your duties require you to speak on behalf of the organisation in a social media environment, you must still seek approval for such communication from your manager. Your manager may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to the Head of Group Services and do not respond without written approval.

Guidelines for Responsible Use of Social Media

When making personal use of social media, (i.e. you are not posting in your capacity as Relyon employee) you must not imply that you are posting on behalf of the company, or as a member of Relyon staff.

Write in the first person and use a personal email address.

Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see. On personal social networks and messaging services– even closed ones like Facebook and WhatsApp – you should be aware that posts can be shared outside of your network. If you make a posting which could bring the company reputation into disrepute then you could be subject to disciplinary action.

If you disclose your affiliation with us on your business based social media profile or in any social media postings, you must state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

You should be aware that it is possible for social media users to connect the work you do for the company with other social media postings. The likelihood of this is increased if you declare on business based social media that you work for Relyon. It is therefore important to remember that when posting in a personal capacity you may still easily be identified by other users as working for the company even if you don't state it.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

The privacy settings on social media apps and websites should give you control over how your personal information is used. All staff who use social media are advised to check their privacy settings before using a particular service and to review them regularly, particularly after any new settings are introduced.

Monitoring

The company reserves 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. This may be done for legitimate business purposes which include ascertaining and demonstrating that expected standards are being met by those using the systems and for the detection and investigation of unauthorised use of the systems.