QA International Certification Limited
Social Media and e-Marketing Policy

Social media policy

This Policy has been prepared by the Directors and Governing Board of QA International Certification Limited (QAICL) and is subject to regular review and update.

This social media policy is made available on an 'information only' basis. QAICL accept no responsibility for the consequences of errors or omissions or any reliance the reader may place on this document when contracting or interfacing with the Company through Social Media.

Introduction

Employees of QAICL may be able to access social media services and social networking websites at work, either through company IT systems or via their own personal equipment subject to terms and conditions of their employment contract.

This social media policy describes the rules governing use of social media at QAICL.

It sets out how staff must behave when using the company's social media accounts and the rules about what staff may say about the company on their personal accounts.

This policy should be read alongside other key policies. The company's internet use policy is particularly relevant to staff using social media. This policy applies to all staff, contractors and visitors at QAICL who use social media while working - no matter whether for business or personal reasons. It applies no matter whether that social media use takes place on company premises, while travelling for business or while working from home.

Social media sites and services include (but are not limited to):

- Popular social networks like Twitter and Facebook
- Photographic social networks like Flickr and Instagram
- Professional social networks like LinkedIn

Responsibilities

Everyone who operates a company social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

The Marketing Officer is ultimately responsible for ensuring that QAICL uses social media safely, appropriately and in line with the company's objectives. The Directors are responsible for providing apps and tools to manage the company's social media presence and track any key performance indicators. They are also responsible for proactively monitoring for social media security threats.

The Scheme Manager is responsible for ensuring requests for assistance and support made via social media are followed up in accordance with relevant Company Procedures and Scheme Regulations.

General social media guidelines

QAICL recognises that social media offers a platform for the company to perform marketing, stay connected with customers and build its profile online. The company also believes its staff should be involved in industry conversations on social networks. Social media is an excellent way for employees to make useful connections, share ideas and shape discussions.

The company therefore encourages employees to use social media to support the company's goals and objectives.

Basic advice

Regardless of which social networks employees are using, or whether they're using business or personal accounts on company time, 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 is 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.** Staff 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. Staff members can always consult the Marketing Officer 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.** Staff members 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, staff 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 QAICL without checking that the company can deliver on the promises. Direct any enquiries to the Marketing Officer.

- **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated enquiries and customer issues. Once a customer has made contact, employees should direct further communications via the Scheme Manager.

- **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.

Use of company social media accounts

This part of the social media policy covers all use of social media accounts owned and run by the company.

Authorised users

Only people who have been authorised to use the company's social networking accounts may do so. Authorisation is provided by the Directors or Marketing Officer. Allowing only designated people to use the accounts ensures the company's social media presence is consistent and cohesive.

Creating social media accounts

New social media accounts in the company's name must not be created unless first approved by the Directors and Marketing Officer. The company operates its social media presence in line with a strategy that focuses on the most-appropriate social networks to the company's business and within available resources.

Purpose of company social media accounts

QAICL's social media accounts may be used for many different purposes.

In general, employees should only post updates, messages or otherwise use these accounts when that use is clearly in line with the company's overall objectives.

Inappropriate content and uses

Company social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the company into disrepute. When sharing an interesting blog, post, article or piece of content, employees should always review the content thoroughly, and should not post a link based solely on a headline.

Use of Employee's own personal social media accounts

QAICL recognises that employees' personal social media accounts can generate a number of benefits. For instance:

- Staff members can make industry contacts that may be useful in their jobs
- Employees can discover content to help them learn and develop in their role
- By posting about the company, staff members can help to build the company's profile online

As a result, the company is happy for employees to spend a reasonable amount of time using their personal social media accounts at work.

Personal social media rules

Acceptable use:

- Employees may use their personal social media accounts for work-related purposes during regular hours, but must ensure this is for a specific reason (e.g. competitor research). Social media should not affect the ability of employees to perform their regular duties.

- Use of social media accounts for non-work purposes is restricted to non- work times, such as breaks and during lunch.

Talking about the company:

- Employees should ensure it is clear that their social media account does not represent views or opinions of the company, the Directors, its staff or customers of QAICL.

- Staff may wish to include a disclaimer in social media profiles e.g. “The views expressed are my own and do not reflect the views of my employer”.

Users must not:

- Create or transmit material that might be defamatory or incur liability for the company.

- Post message, status updates or links to material or content that is inappropriate. i.e. content that includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs. This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

- Use social media for any illegal or criminal activities.

- Send offensive or harassing material to others via social media.

- Broadcast unsolicited views on social, political, religious or other non- business related matters.

- Send or post messages or material that could damage the company’s name, image or reputation.

- Interact with QAICL's competitors in any ways which could be interpreted as being offensive, disrespectful or rude. Communication with direct competitors should be kept to a minimum.

- Discuss colleagues, competitors, customers or suppliers without their approval.

- Post, upload, forward or link to spam, junk email or chain emails and messages.

Security of information and data protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

Users must not:

- Share or link to any content or information owned by the company that could be considered a breach of confidentiality or impartiality regulations or otherwise post information deemed to be commercially sensitive. This might include sales figures, details of customers, or information about future strategy or marketing campaigns.

- Share or link to any content or information owned by another company or person that could be considered confidential or commercially sensitive. For example, if a competitor's marketing strategy was leaked online, employees should not mention it on social media.

- Share or link to data in any way that could breach the company's data protection policy.

Protect social accounts

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

- Staff must not use a new piece of software, app or service with any of the company's social media accounts without receiving approval from the Directors or Marketing Officer.

- Staff 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.

Policy enforcement

Monitoring social media use

Company IT and internet resources - including computers, smart phones and internet connections - are provided for legitimate business use. The company therefore reserves the right to monitor how social networks are used and accessed through these resources. Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all data relating to social networks written, sent or received through the company's computer systems is part of official QAICL records.

The company can be legally compelled to show that information to law enforcement agencies or other parties.

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment. Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

For and on Behalf of the Directors of QAICL: 08 August 2016