Guidelines

For ScaleAQ employees online and in social media

1. INTRODUCTION

Social media such as Facebook, Twitter and LinkedIn have become an important communication channel for both individuals, companies and public institutions. For businesses, social media offers many opportunities and some challenges. In order for us all to have a common and mutual understanding, we have established some guidelines and recommendations for the use of social media – on behalf of the company and as a private individual.

2. THE COMPANY IN SOCIAL MEDIA

2.1 Introduction

ScaleAQ is – and should be – visible in social media.

2.2 Who makes a statement on behalf of the company?

Statements and posts on social media on behalf of the company should only be made by persons authorized to do so.

2.3 The content of the communication

In all communication on social media on behalf of the company, the following must be taken into consideration:

- Our values should be the basis for all communication.
- We must present ourselves with openness and transparency.
- We must always be honest and speak the truth.
- We must act with care and be informative and professional.

All communication must be within the law, regulations and agreements. We shall:

- Respect copyright and individual privacy.
- Avoid privacy violations.
- Not disclose sensitive or confidential information.

3. PRIVATE USE OF SOCIAL MEDIA

Private use of social media is up to the individual and belongs in the private sphere. The company respects the individual's freedom of expression, *but also wishes to give a reminder of the duty of confidentiality (see the employment agreement).* However, based on our line of business, we would like to make some recommendations and guidelines for private use. Below you will find some informal rules that may be useful.

3.1 Private use and identity

Think about your personal digital footprint. What you yourself publish on social media spreads easily and often remains visible and searchable for a long time, often for several years.

Avoid any doubts and ambiguities about your identity that may contribute to unnecessary confusion. Write that you are employed by ScaleAQ if applicable. You should be open about working in ScaleAQ, and you must clearly mention that you are a private individual with your own opinions. If you have not agreed otherwise with your manager, you represent yourself, not the company. Write in first person so that it is clear that you are expressing yourself as a private individual.

3.2 Listen first

All social media has its culture of expression. Find and understand the rules, perceptions and needs of the online community you are addressing before you get involved.

3.3 Decide what you want to say

It is important to be conscious of what you want to express. Act delicate, informative and professional. Remember that your content may be visible to everyone, even if you publish the content within a closed circle. Do not post content what is harmful to the reputation of others or yourself.

Many people later regret what they have posted (see www.slettmeg.no).

3.4 Avoid mentioning business-related matters

Discuss challenges about issues that directly relate to the job with your manager – not online. When it comes to our job, we should not mention:

- Business-sensitive and confidential topics.
- Our colleagues and leaders.
- Customers, suppliers and partners.
- Specific tasks
- We should not “check in” at companies we are visiting. Depending on the case, this may actually be sensitive information.

3.5 Be open

Appear with openness and transparency in social media as in other contexts.

3.6 Respect your readers

Share your knowledge and experience. Respect the views of others and avoid contributing to conflicts.

3.7 Take responsibility

If you have made a mistake, it is often a good strategy to admit the error, apologize, and help correct it.

4. DON’T BE FOOLED

Social manipulation utilizes human contact and social abilities to obtain or influence information. Business secrets, personal data and information about IT systems can be valuable to others and abused for fraud or criminal acts. The attacker often acts respectfully and may, for example, pretend to be a repairman, new employee or operations manager. He often collects information from one source to build trust with the other.

General precautions:

- Be skeptical of spontaneous requests.
- Try to get people’s identity confirmed.
- Do not disclose information that the recipient is not entitled to.

Also, be critical of what is written on social media. The information is not always fact-based, but the opinions or understanding of individuals.