IMC Worldwide Ltd. Social media policy

IMC Worldwide is committed to utlising available technology and innovation in order to improve the efficiency and effectiveness of our business. This includes using a variety of means to improve the way we communicate with our partners, clients and the development community.

'Social media' is the term commonly given to web-based tools which allow users to interact with each other either by sharing information, opinions, knowledge or interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement. Whilst this offers new and creative ways for us to interact, the application of new technology means there are a growing number of data security, libel, and confidentiality issues to consider.

To avoid major mistakes which could result in reputational, legal and ethical issues it is important that we manage any potential risks through a common-sense approach and framework as well as proactively monitoring the development of such applications.

These guidelines should be read in conjunction with any information provided by the Communications team on the use of social media.

1 About this policy

1.1 This policy is in place to minimise the risks to our business through use of social media.

1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

1.3 This policy covers all employees, officers, consultants, contractors, interns, and agency workers.

2 Personnel responsible for implementing the policy

2.1 Our board of directors (the board) has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to IMC’s IT Director.

2.2 Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with IMC’s IT Director who will review this policy annually to ensure that it still responds to the latest technology developments, that it meets legal requirements and reflects best practice.

2.3 Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

2.4 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to IMC’s IT Director.

Questions regarding the content or application of this policy should be directed to IMC's IT Director.

3 Compliance with related policies and agreements

3.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to breach IMC Policies, including:

I. Security policy, principles and guidelines;
II. Ethics and anti-corruption policy and guidelines;
III. Acceptable IT and computer use;
IV. IT security policy;
V. Data protection policy; or
VI. Breach any other laws or regulatory requirements.

3.2 Staff should never provide professional or character references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the organisation.

3.3 Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

4 Personal use of social media

4.1 Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

5 Prohibited use

5.1 You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

5.2 You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

5.3 You must not express opinions on IMC's behalf via social media, unless expressly authorised to do so by your manager. You may need to compelte a briefing session with the Communications team - in order to obtain such authorisation.

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

5.5 The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment you must provide us with a copy of all such information.

5.6 Any misuse of social media should be reported to IMC's IT Director.

6 Business use of social media

6.1 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 line manager, who may require you to have a short briefing from the IMC Communications team or undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

6.2 Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to IMC's IT Director and do not respond without written approval.

7 Guidelines for responsible use of social media

7.1 Respect, responsibility, and good judgement are the foundations of safe and productive use of social media.

7.2 IMC works in countries worldwide, some of which are fragile and conflict-affected states in which safety and security of our project teams may be compromised by improper use of social media—for example, photographs posted to a social media account may include geotagging meta data that can publicly highlight your location or the location of others in the photograph, which may in some cases compromise the safety and security of those in the photograph.

7.3 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address.

7.4 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.

7.5 Always ask permission before posting content relating to another individual to a social media account. The safety and security of that person may be compromised by irresponsible social media use.

7.6 Photos of children should not be published to social media without the express permission of their parents or guardians.

7.7 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out in paragraph 5.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

7.8 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 (or Project Manager, if an indepednent consultant or sub-contractor).

7.9 If you see social media content that disparages or reflects poorly on us, you should contact your line manager (or Project Manager, if an indepednent consultant or sub-contractor).

8 Monitoring

8.1 We reserve 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, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

8.2 For further information, please refer to our Acceptable IT & Computer Use Policy.

9 Recruitment

9.1 We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

10 Breach of this policy

10.1 Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

10.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Partner organisation or independent consultant commitment to this policy:

Name of Firm if applicable: ______________________________

Signature: ______________________________

Full Name: ______________________________

Position in organisation if applicable: ______________________________

Date: ______________________________