Social Media Policy

1 Purpose
Social media such as Facebook, Twitter, Blogs, LinkedIn, YouTube and many more, play a crucial part in today’s communication. Unlike the classical analogue media, they allow all users to create, share and promote their views to a broad public. It is no secret that social media has great potential for campaigning and for shaping public opinion. However, the flip side of the coin is that there are many pitfalls, especially regarding all aspects of security and reputation on a personal and a corporate level. This is why all employees are encouraged to use social media responsibly when communicating about topics within their areas of expertise.

This policy provides rules and helpful, practical advice on the “private” use of social media accounts in order to protect ICMPD’s employees as well as to safeguard ICMPD’s reputation.

If you have any questions, please contact the Communications Unit: media@icmpd.org

2 Scope
This policy is binding for every ICMPD employee, who is or plans to become active on any social media platform, such as Facebook, Twitter, Flickr, YouTube, Instagram, LinkedIn and other social media, including blogs.

As laid out in the Code of Conduct (“Individual responsibilities”) every staff member has agreed to “protect and enhance ICMPD’s brand reputation...” and to “...coordinate communication activities involving the media with the Communications Unit...”

Employees subject to a Special Service Agreement (SSA) are bound by the Code of Conduct section of the General Conditions, which they agreed to when signing a contract with ICMPD1.

3 Recommendations for safe and conscious use of social media

3.1 Be a good ambassador. Your behaviour always reflects on the organisation. Keep the Code of Conduct in mind.

3.2 Rule of thumb: Do not say or write anything that you would not be comfortable seeing quoted in a newspaper headline or having to justify to your supervisor. If the information you are about to post makes you feel uncomfortable, do not post it. Consult with your supervisor and with Communications in case of doubt.

---

1 “The Subscriber shall, in particular, refrain from making any public statements concerning the relevant project or services and/or from direct contact with project Contracting Authorities/donors, other than provided for in his/her Terms of Reference, without the prior approval of ICMPD, and from engaging in any activity which conflicts with his/her obligations towards ICMPD and the Contracting Authority.”
3.3 **Personal does not mean private.** While it often seems as if you are private when acting on social media this is rarely ever the case. It is easy to track private conversations through Google searches, even if you have not fallen victim to a cyberhack. That is why you should always be considerate when communicating through these channels and keep in mind that “personal is not private”.

3.4 **Factual information:** When engaging in online discussions about ICMPD or topics we deal with, you might want to correct someone else, but make sure you only provide factual information you can prove.

3.5 **Do not “feed the troll”**. Sometimes, you will find that someone intentionally misunderstands you in order to provoke you – in this case the “do not feed the troll” rule applies. Ignore that person and do not get emotional about the incident.

3.6 **Be the first to admit a mistake** – and be upfront about it. Remember that the “internet never forgets anything”, so, if some information was really wrong, someone has noticed and taken a screenshot. You can proactively communicate about the mistake and the changes that were made in order to correct it.

4. **Rules**

4.1 **Code of Conduct:** The Code of Conduct applies to the digital world and your activities on social media.

4.2 **Speak only for yourself.** Use a disclaimer to make clear you are not speaking on behalf of the organisation. Only ICMPD authorised, official accounts are entitled to speak on behalf of the organisation.

4.3 **Do not use logos and emblems** or screenshots of ICMPD products as your personal profile or header photos. Not only does this imply that you are an official ICMPD spokesperson/authorised social media account, it also goes against our copyrights and those of our partners.

4.4 **Only tweet or comment on projects if you are directly working on them and if there was no restriction to communicate on the project.** In case you would like to comment on or promote another ICMPD project that you are not working on directly, please do so only by **using the retweet function** without any comment. This type of retweets is highly encouraged. If there has been no communication on certain project outcomes, actions or meetings by an authorised official account yet, wait until the authorised accounts go out with the information. **The same principle applies to all other social media channels.**

4.5 **Respect privacy and image rights**: You must have consent from every person that you are showing in a photo and can clearly identify. The only exception to this is in a public street scene where you do not focus on any particular person but only photograph “the street”.

4.6 **Setting up project accounts** and accounts where ICMPD is a consortium partner: Projects that wish to set up a social media account must always consult with the Communications Unit first. It is the only way to ensure consistency and support from the Communications Unit.

4.7 **Protect your privacy.** Lock screens when devices are not in use. Set passwords with a high security level, never share them and change them regularly. Select settings where you restrict who can see your personal information. Whenever possible, avoid linking and synchronising apps since you lose control over what can be found on the web. Staff members, personnel and interns must adhere to ICT policies and rules.

4.8 **Travel and security:** As ICMPD becomes better known, it also becomes increasingly vulnerable to security threats from different groups. It is extremely important not to post any information which

---

2 See *European Court of Human Rights Factsheet on the Right to the Protection of One’s Image*: https://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf
may have an impact on the security and safety of ICMPD employees, ongoing and future activities, and assets of the organisation. For instance, exact dates and times of missions and events in high-risk areas.

**Further relevant documentation**

- *Policy on Computing and Information Technology Facilities*
- *Guidelines for Account Management*
- *Code of Conduct*
- *SSA General Conditions*