The Institute
of
Fire Safety Managers

Established 1997

Social and Digital Media Policy

Version: 1

Summary:	This policy looks at the use of social and digital media, the guidelines to follow when on the official Institute's channels and it also sets the guidelines for Council, staff and members when active on their own accounts.	
Target Audience:	Council, Staff & Members	
Next Review Date:	December 2025	
Approved by:	Directors	05/12/22
Ratified by:	Council	19/12/22
Date issued:	December 2022	

Table of Contents

1. Introduction

Social and Digital Media are powerful tools to engage members, potential members, employees and general public. As it creates the opportunity to champion the Institute's brand and increase awareness of fire safety. We support the appropriate use of Social and Digital Media platforms but are mindful of the risks and responsibility these bring.

When using such platforms in a personal or professional capacity it is crucial that employees, Council and members act and behave in the correct and appropriate way as not to disclose confidential information, incorrect advice or damage the Institute's reputation. These guidelines and guidance set out the standards of behaviour and practices we expect from all employees, Council and members when using Social or Digital Media platforms.

The policy covers the use of **Digital Media** – Internet sites, intranet sites, apps and other online environments e.g., Teams, OneDrive and **Social Media** – Technology that enables users to interact, create external communities and share information online. This includes (but is not restricted to):

a) online communities and chat forums e.g., Facebook, LinkedIn
b) interactive websites e.g., Twitter, that allow users to comment, blog and micro-blog.
c) content-sharing sites e.g., Instagram.
d) wikis; and
e) social networking.

This policy is enacted under the bylaws of the Institute and in conjunction with other IFSM policies and standards, including the Code of Ethics, Employee Handbook and Data Protection Policy. If behaviour online would violate an IFSM policy in another forum, it will also violate it on social media. Employees, Council and members who violate this or other IFSM policies may be subject to disciplinary action up to and including termination of their post / employment.

2. General use of Social and Digital Media

Those who use Social or Digital Media for their personal use – during or outside working hours and using the Company's equipment or their own – should exercise good judgement, and consider the potential risks and consequences of their actions and of any content they post online. Their Social and Digital Media presence is a reflection not only of themselves, but of The Institute as well. They are responsible for anything they have posted on Social and Digital Media that could potentially harm the Institute's reputation or that of our partners, customers and suppliers, whether or not they identify themselves as a an employee or Council member in their Social or Digital Media profile.

You must never use Social or Digital Media to post or display information, images or videos about the Company, our partners, customers or suppliers, or the people they work with, that could be considered:

a) misleading or otherwise untrue;
b) vulgar;
c) obscene;
d) threatening;
e) intimidating;
f) disparaging;

g) harassing;
h) libellous;
i) demeaning or discriminatory on the basis of age, race, religion, sex, sexual orientation, disability, national origin, ethnicity, marital status, or any other legally recognised protected basis under the applicable law.

You should not use IFSM email address to set up personal Social or Digital Media accounts unless the account is related to work.
Failure to follow these guidelines may result in disciplinary action, up to and including dismissal, in line with the relevant Disciplinary Policy.

2.1 Using multimedia

Think carefully before sharing photos and videos – not everyone is willing to have their images posted on the internet, and you may risk breaking the law by posting photographs of individuals without considering privacy implications. You should always ask for permission before you post someone's picture on a website.

2.2 Observe Copyright Rules

If you copy a photograph, a video or a piece of music from a third party website (or any other source), and use it without permission from the copyright owner, this is likely to be an infringement of copyright. The fact that the work is published on the internet and available to the public makes no difference. It should also be noted that acknowledging or providing attribution to the copyright owner does not bypass copyright law. You should always try to use material from approved public Social and Digital Media channels in the first instance.

2.3 Engaging with Social and Digital Media accounts

It may be appropriate to tag employees, Council and members in posts. Gain prior approval from them, don't assume approval, regardless of how active an employee is on Social or Digital Media (whether personal or Company-focused).
Social and Digital Media is all about sharing information and connecting with people. Think before you link – ask yourself whether an online connection is appropriate before asking a colleague to connect with you on Social or Digital Media. Employees may not feel comfortable with friend requests from their manager and similarly managers may be uncomfortable with friend requests from their team members.

2.4 IT security

External Social and Digital Media sites are frequently used for harvesting information, installing spyware and distributing malware. Malicious activity includes 'phishing', 'pharming', identity theft and other more serious crimes. Be extremely careful when opening attachments from unknown sources, clicking on hyperlinks from untrusted senders or downloading anything from Social and Digital Media sites.

Remember, the information you publish may be seen by other web users for a very long time, even if you delete it. Anything you share can be forwarded on and may potentially remain available forever, even if you have enabled privacy and security settings.

2.5 Messaging Services

The lines between Social and Digital Media and peer to peer messaging have blurred. Messaging now predominantly takes place via internet based external platforms. Either dedicated messaging services such as SMS, WhatsApp and Teams or integrated into existing Social and Digital Media platforms such as Facebook Messenger and direct messages on Twitter.

SMS, Whatsapp and Teams are great tools for keeping in contact with colleagues where applicable, other messaging applications, like Facebook messenger and Snapchat are appropriate for social use only.

Employees are reminded that the use of personal phones are not allowed during work hours and these applications should be used for company business using company devises.

3. Posting about the Institute on Social and Digital Media

We publish content about the work we do and information to benefit fire safety. We encourage employees, Council and members to retweet, share, like and comment on our Social and Digital Media posts.

Employees, Council and Members may post or share information about the Institute on personal Social and Digital Media that has been **approved for public release** by the Institute. This **could** include:

a) Information that is published on our website or Social and Digital Media channels;
b) public news releases;
c) electronic brochures or marketing materials;
d) external job postings; or
e) photos or information from a public event.

It is important to remember that content discussed within the office or in meetings is intended for internal use only, and **is not approved** for public release and should not be shared on Social and Digital Media.

If employees create their own content, any information relating to The Institute should be based upon information already approved for public release and any personal opinion or commentary on this information should be clearly identified as such. In particular, employees should not share any confidential Company information, information intended for internal use only or information about a private company event.

If an employee, Council member or member visits an event either hosted by the Institute or attended by the Institute, they may post Social and Digital Media content related to their participation, but should exercise caution and ensure they follow the guidance on general use of Social and Digital Media.

3.1 Expressing your personal views about The Institute and Industry Information

Whatever your role in the Institute, your Social and Digital Media presence is a reflection not only of yourself, but also of the Company. Anything you post or share that could potentially harm our reputation is ultimately your responsibility. This is especially true if you identify as an IFSM employee, Council member or member in your Social and Digital Media profile. You can identify your involvement with The Institute if you would like to but think carefully before posting and make it clear your views are your own.

You are advised to write in the first person ('I' rather than 'We' or 'The IFSM) to show that you are speaking for yourself and not on behalf of the Company.

You are advised to use a disclaimer, such as 'The views expressed on this site are my own and don't reflect the views of The Institute of Fire Safety Managers and are given with out prejudice'. Remember, even if you use a disclaimer, your behaviour and comments are still subject to the Social and Digital Media Guidelines.

Be mindful of your professional indemnity insurance with any advice or opinions you give on social media. The Institute or individual could end up being challenged in a court of law for advice given. The Institute only ever answers genetic queries via email, with the caveat that we are not a technical query answering service and any advice or answers are given without prejudice.

3.2 Participating in conversations.

Sharing personal views and positive experiences can help promote the Institute brand. Caution should be exercised.
Be an informed voice in online conversations and use publicly available facts and information to support your viewpoint or experience.

3.3 Responding to criticism

If you come across criticism and it is cause for concern report this to the Business Manager. If it is not cause for concern and you want to reply, please use publicly available data/facts from open Company publications or the internet, or your own positive personal experiences.

Make sure you are rational and in control, never contribute to a discussion if you are angry. Wait, calm down and return to it at a later date.

Stay calm and don't pick fights by escalating heated discussions. Be conciliatory, respectful and quote facts to pacify the conversation and correct misrepresentations.

4. Posting on behalf of The Institute using official Company channel

The official Institute's branded Social and Digital Media sites and channels have been established or approved by our Marketing and Publications subgroup. They enable us to engage with key audiences and online communities and enter into dialogue about our products, services and industry news. All new channels should be approved, in advance, by the Marketing and Publications subgroup. They will be reviewed regularly by the Marketing and Publications subgroup to ensure that they are still required and are meeting their objectives.

All official Social and Digital Media sites and channels are subject to control and direction from the Marketing and Publications subgroup even when not run day-to-day by them. Only authorised representatives of the Company may post approved content and information using these channels. The Marketing and Publications subgroup has the right to remove any Company account or content at any time.

4.1 Engaging with external Social and Digital media content

Sharing third-party information or links on Social and Digital Media could result in the content being attributed to (and considered as endorsed by) The Institute. Exercise the same caution as if you were creating an original post.

Review associated channels and previous content when you like, share or re-tweet third-party content or links.

4.2 Responding to information requests

You may receive requests for information through various channels. Respond to requests using information that has been approved for external release. All technical queries should be made via email.

5. Monitoring and Reporting issues

It is important to monitor our Social and Digital Media presences to track and manage public comments.

If you have any concerns or issues about using Social and Digital Media you can speak to your line manager, the Business Manager or the Marketing and Publications subgroup.

If you see a post or comment by an IFSM employee on Social or Digital Media that you are concerned about you should report it to your line manager.

If you see misrepresentations or false statements about The Institute on Social or Digital Media and want to reply, please use publicly available data/facts from open Company publications or the internet. Please also report this to the Business Manager.

The Institute has the right to monitor all Social and Digital Media activity undertaken when using Company IT equipment. The Company may also view Social and Digital Media content on an employee's personal pages that is publicly available, or private content if brought to their attention by another person who has access to that content.

Employees should be aware that they may be asked to remove Social or Digital Media posts that the Company considers inappropriate.

As a rule if you are unsure whether to post something or respond to a post then DON'T. Seek advice.

Version Control

Change Record

Date	Author	Version	Page	Reason for Change

Reviewers/contributors

Name	Position	Version Reviewed & Date