

# Social Media Guidance, 3M UK & Ireland

---

*“What I do in my own time on my own computer can’t possibly lead to disciplinary action being taken against me by my employer”*

Wrong

## Overview

We live in an electronic age, where the boundary between our business and personal lives has become rather blurred. For many of us, just a few moments on Google is all that is needed to identify us as 3M employees. If you have a LinkedIn profile, for example, you have probably named 3M as your employer.

There is nothing at all wrong with that – the vast majority of us are proud to be 3Mers. However, we need to be aware that in the cyber world our personal thoughts have the potential to be interpreted as being representative of 3M’s views.

It is a complex issue and the possible pitfalls are many and varied. This guidance is designed to highlight the potential issues we face as employees – and help avoid damage to both the company’s reputation and individuals’ careers.

This guidance has been created for the UK and Ireland as an addendum to the global [3M Social Media Standards for Business Use](#) and [Personal Use of Social Media Standard](#).

## Social media guidance

The internet enables us to participate in interactive discussions and share information using a wide variety of social media, such as Facebook, LinkedIn, Twitter, blogs and wikis. However, employees' use of social media can pose risks not only to 3M’s confidential and proprietary information, but also the company’s reputation. To minimise these risks, employees should adhere to company policies and follow this guidance.

It applies to the use of social media for both business and personal purposes, whether during business hours or otherwise, and whether employees are using 3M equipment or their personal phone or computer.

3M reserves the right to monitor any business social media activity and any personal social media activity, where it is in the public domain.

Any breach of company policies may result in disciplinary action, up to and including dismissal.

This guidance covers not only the business use of social media, but also personal use, where this is in the public domain. This guidance is formed of two parts:

1. Business use of social media
2. Personal use of social media.

Any situations not covered in this guidance should be checked through the Social Business Manager to ensure compliance and support future guidance development.

## **1. Business use of social media**

Whenever conducting business on behalf of 3M, you are required to comply with all 3M Business Conduct policies. Always represent 3M ethically, with professionalism and integrity.

When recruiting agency staff or contractors to manage any of 3M's online channels, please ensure that they also comply with this guidance.

All persons engaged to work on behalf of the company are responsible for protecting the confidentiality of 3M information. Do not speculate about or share intellectual property or confidential, financial, operational, strategic, personnel or customer information, trade secrets or any other information that would represent a violation of 3M's corporate policies.

Protect the reputation of the company, its employees and contingent workers, as well as customers and all business relationships.

In order to conduct any business as a representative of 3M on social channels, you must first complete mandatory training delivered jointly by the Corporate Communications and Social Business teams. *This covers the need to act with caution, the need to be respectful of others' legitimate views and the importance of reporting any public relations concerns, for example, defamatory or untrue statements being made about 3M, our employees or representatives. A checklist will be provided with training that must be used to check all published content. As a matter of good practice all blog entries should be double-checked prior to posting by a colleague who has received formal social media training.*

All employees responsible for online business channels must provide the Social Business team with access to their sites to enable them to be monitored. Managers of social channels must also arrange for moderation to continue during any periods of absence.

A moderation protocol must be established for all businesses, including provision for out of office hours' monitoring and escalation procedures for issues or crisis situations. This must accommodate queries that come in through central channels or social listening, so not having a business page does not exclude a business from requiring a process.

If you see online content that disparages or reflects poorly on 3M organisation or stakeholders contact Corporate Communications and/or the Social Business team.

### Official 3M social media sites

Formal naming conventions apply when setting up a channel in 3M's name. Seek guidance from the Social Business team before creating an official Facebook, Twitter or other social media site.

Use a managed 3M generic email addresses ([available via IT Security](#)) on all public information or comments, as well as on online business channel logins.

Use secure passwords, employing a combination of upper and lowercase, numbers and characters. Do not use a password that can be recognised as a word. If your channel is hacked, change your password immediately. Apologise to followers if they may have been affected.

Comply with 3M's Brand Identity Standards on 3M managed channels on external platforms. See [www.3M.com/identity](http://www.3M.com/identity) for further information.

All business activity on social channels must comply with the [CAP code](#), [ABHI Code of Business Practice](#) (where appropriate) and [Facebook page guidelines](#). Legal advice can be obtained from the [Institute of Promotional Marketing](#) – contact the [Social Business Manager](#) for details of our consultant.

Do not remove or delete posts where complaints are made. The internet is permanent and transparency is encouraged. Always seek advice from Corporate Communications and/or the Social Business team when dealing with an issue or crisis.

## **2. Personal use of social media**

As a 3M employee, you may be identifiable as such through social media (for example, your LinkedIn profile or your Facebook 'About' section). Accordingly, you are personally responsible for taking sensible precautions to protect the company's reputation.

Where there could be any doubt, ensure you state in your personal information that your opinions are your own and not that of your employer.

When providing references, such as recommendations on LinkedIn or similar platforms, be clear that this is from you as a personal individual and not from 3M (for example: "These views are personal to me and are not contributed on behalf of my employer.")

Use your personal email address for personal communications. Never use your official 3M email address for such messages.

Never post unwelcome or derogatory remarks about colleagues, customers or suppliers.

Comments made on social networks which affect the dignity of a colleague at work could be deemed as harassment, regardless of whether such comments are made during or outside of working hours.

Never enter an online discussion about work matters without identifying yourself as a 3M employee. If you are not authorised to represent 3M online and have concerns about any posting, please alert the Corporate Communications or Social Business teams.

Do not make comments that could damage 3M’s reputation or the reputation of 3M employees, contingent workers, customers and other business relationships. Avoid communications that could damage our company’s reputation, even indirectly.

Disciplinary action may be taken if there is violation of 3M standards or the company is brought into disrepute.

All employees should be aware that information may be gathered from online sources for [‘social engineering’](#) purposes and used in an attempt to build trust and gain access to company confidential information. Any suspicious phone calls or emails should be reported to the [Safety and Security Manager](#).

## Related policy information

[3M Social Media Standards for Business Use](#)

[Electronic Resources Policy](#)

[Business Conduct and Ethics at 3M](#)

[Electronic Resources Policy](#)

[Reference Policy](#)

[Information Security Policy](#)

[Personal Use of Social Media Standard](#)

[Harassment Policy](#)

[Suspicious Phone Calls to 3M](#)

## Further information

Social Business: [Kirstie Heneghan](#), [Nicole Pritchard](#), [Philippa Chesters](#)

Corporate Communications: [John Klee](#), [Ros Smith](#)

Safety and Security Manager: [Simon McKenna](#)

## Revision date

Last revised 23 January 2013

As a contingent worker at 3M I understand that I am required to follow this guidance in the same way as permanent employees of the company. I have read, understood & will comply:

.....

Signed:

Date:

Name: (please print)