

Top 10 tips for social media use



Social media platforms such as Facebook and Twitter can be vital tools for practices looking for an effective way to communicate with patients. But there are risks to consider before taking the plunge. From confidentiality and data security to negative feedback and professionalism, below are 10 tips covering the most common risk areas.

1. **Have a social media policy in place.** This should detail what is expected of staff members when using social media for both work and personal purposes. For business channels, make it clear which members of staff can contribute and the type of content that should be posted/shared. If you choose to open your platforms to third party comments, have processes in place for responding. When it comes to employees' personal social media accounts, clearly outline the type of behaviour that is deemed acceptable. They may be using these sites while "off duty", but they are representatives of the practice and must behave professionally and responsibly.
2. **Think about what you want to communicate to your audience.** Share and post content that is both relevant and beneficial to your patient population. Patients are much more likely to engage if they find your content relatable.
3. **Maintain patient confidentiality.** At no point should you share or discuss an identifiable patient's care on social media without their explicit consent to do so – this applies to both business and personal social media use. Be cautious even if a patient isn't explicitly named as they may still be identifiable; if in doubt, seek consent. If you are sharing videos/photos from the practice without explicit consent, ensure no patient identifiable information is visible and that there is no way in which the patient could be identified.
4. **Regularly review your social media page's privacy and security settings.** To minimise the risk of being 'hacked' you should change your password regularly and, if accessing practice accounts on personal devices, make sure those devices are password protected at all times. Keep up-to-date with any changes to terms and conditions made by social media platforms that you use.
5. **Agree with GP partners the extent to which patients will be able to engage with you on social media.** Your presence should be public but carefully consider whether to allow patients to comment publicly on your posts, message you privately or 'tag' you in their own private posts.
6. **Check reliability of sources when sharing content.** To avoid spreading incorrect or misleading information, only share posts from verified sources. Exercise caution: if something evokes an emotional response with you, or does not sound plausible, research further.
7. **Be wary of responding to online criticism.** As frustrating as it is, it is almost always best to avoid responding online to negative comments or criticism unless via a formal channel such as NHS Choices. Doing so risks breaching patient confidentiality and may also exacerbate any perceived grievance. If you do decide to respond, keep it concise and professional. Consider inviting the individual to contact you directly to discuss the matter in a more appropriate setting and follow GMC advice within their guidance on *Responding to criticism in the media* [here](#).
8. **When using group chats with the practice team, be sure to set limits.** As useful as group messaging on platforms such as WhatsApp can be, it is not reasonable to expect staff to engage outside working hours. Make sure staff know when it is appropriate to 'mute' conversations and how to do so. You should also have a clear policy on the type of messages that should be sent – remind the team to remain professional, not to share patient identifiable information, and not to send images/jokes/comments that could cause offence.

9. **Be mindful of security when using social media/online platforms for work meetings.** Only share the login details and any passwords of meetings with those who are required to attend and where possible 'lock the room' when everyone is in attendance to avoid unauthorised access from a third party.
10. **Follow General Medical Council guidance.** There is clear regulatory guidance on *Doctors' use of social media* [here](#), which should be followed whether using social media in a personal or professional capacity.

More detailed guidance on the personal and professional use of social media is available in the advice library at www.mddus.com

MDDUS Mackintosh House 120 Blythswood Street Glasgow G2 4EA
T: 0333 043 4444 • E: risk@mddus.com • W: www.mddus.com
Twitter: @MDDUS_News

MDDUS is not an insurance company.
All the benefits of membership of MDDUS are discretionary as set out in the Articles of Association.

Note: The information in this document is of general application only and members are encouraged to seek the advice of an MDDUS medical or dental adviser on 0333 043 4444 if in any doubt.