NOT PROTECTIVELY MARKED
Procedure owned by OSDG

Social Media - Hints, Tips and Other Useful Information

WARNING - THIS INFORMATION HAS EXPIRED
Please contact the OSDG department

Basic principles

There are some basic principles you should follow when using digital technology as part of community engagement:

Be 'Credible' - Experience shows that communities like engaging with Police Officers and staff, especially those working at the frontline. Be accurate, open, fair, honest and transparent in what you write.

Be 'Consistent' - Encourage constructive feedback and discussion. Be professional and honest - friendly but not familiar.

Be 'Responsive' - Wherever possible respond to content posted by others, whether positive or negative. This is your chance to reflect the real situation and communities will value honest feedback. If someone posts something inappropriate, remove it as soon as you see it, keeping a record of what was said, by who and when.

Be an 'Ambassador' - Remember that you are an ambassador for your Force and the Police Service as a whole. As such you are expected to exercise sound judgment and common sense.

Be 'Inclusive' - Remember that not everyone has access to the internet. Digital engagement is an additional tool to use but make sure you have a range of ways to engage with communities. Make sure you continue to highlight key messages to communities through newsletters, public meetings and street briefings as well.

Be 'Ethical' - Information posted online should not:

- Contain protectively marked or otherwise sensitive information
- Disclose unauthorised personal information
- Be libellous
- Breach copyright
- Undermine operational activities
- Damage the reputation of the Police service

Generally, you should not post any information or messages on the internet that you would be unwilling to release to the press or say at a public meeting.

Be 'Personable' - Officers should ensure their sites are engaging and interesting for the audience using the site. Neighbourhood Policing is delivered by personalities within communities and the online personality should reflect the Officer whilst working to Staffordshire Police values.

Time

All accounts must be checked regularly but within reason. It should only take 5-10 minutes to check messages, wall posts and add updates. If you have many messages to reply to this will understandably take more time so please use reasonable judgement.

If you know you will be on rest days / annual leave for a period of time and will be unable to check your account, please make sure another member of your team has access.

When responding to messages, please ask the messenger to contact you using your work email address if you need to continue the conversation, as Facebook messaging does not go through the secure system our emails use.

Twitter tips

- Don't just use Twitter to broadcast - think about engaging.
- Start looking for opportunities to engage - if people are posting on Twitter on a relevant subject they are looking for people to engage with them.
- Ensure that your tweets are adding value.
- The big thing which will start to raise your profile is hashtags - use the right hashtags (#police and #staffordshire seem relevant), I'd start using location specific hashtags like #springfield.
- Who else is using Twitter in your area? Look for local websites who use Twitter - search on the #staffordshire tag and engage with them.
- Use RT (re-tweet) for interesting and relevant tweets.
- Use www.bit.ly to shorten links. You only have a limited number of characters on Twitter and long URLs can soon

use them up. Bit.ly will provide a short link that redirects to the original.

- If you have mobile access use Twitter when you're out on the streets doing something in/with the local community "I'm speaking with the boys and girls at St Peter's School about being safer in their neighbourhood #police #stafford #high street bit.ly?xhmt09s"
- Start sharing your Twitter details when engaging - word of mouth is great
- Think about twitpics, people love them!
- Finally, start following more people than each other - don't worry about direct messaging - there are ways around this, if you get spam followers block them.
- Follow people who follow you, but make sure you take a moment to review them. Are they from the local community, or are they serial followers i.e. They are following several thousand others for no apparent reason.
- Remember your followers can see who you are following and who else is following you. Sometimes it will be advisable to block someone who follows you.

In conjunction with the Communications Team, conduct a period review of your followers and those following you, ensuring they suit the purpose of the site.

Glossary of Twitter terms

Twitter overview

Twitter is a 'microblogging' platform which allows users to post short text messages (up to140 characters in length) and converse with other users via their phones or web browsers. Unlike email or text messaging on mobile phones, these conversations take place in the open.

The platform is experiencing a phenomenal adoption curve in the UK and being used increasingly by government departments, Members of Parliament, a number of our stakeholders as well as millions of businesses, non government organisations and individuals. It is free to use with a relatively low impact on resources and has the potential to deliver many benefits in support of our communications objectives.

Twitterverse or **Twittersphere** or **Statusphere** - the universe / world sphere of Twitter (cf. blogosphere)

Tweet – an update on Twitter, comprising a message of up to 140

characters, sometimes containing a link, sometimes containing a picture or video. Also a verb: to tweet, tweeting.

Reply or **@Reply** – a message from one user to another, visible to anyone following the user who is giving the reply. Also visible to the entire world (and search engines) in your Twitter profile page.

Direct message or **DM** – a message from one user to another in private (not visible to other users, the internet or search engines).

Re-tweet or **RT** – repeating a message from another user for the benefit of your followers and in recognition of its value (the Twitter equivalent of forwarding an email)

Twitter client or **application** – software on your mobile phone or computer that you use to access Twitter. Popular clients are the Twitter website itself, Tweetdeck desktop software and a number of iPhone applications.

Micro-blogging – the term given to the practice of posting short status updates via sites like Twitter (there are others, but none as big)

Follower – someone who has subscribed to read your tweets. Displayed on Twitter as:

"Following" The people that you follow on Twitter
"Follower" Someone who follows you on Twitter
"Friend" Someone who you follow that also follows you.

Twitter API – Twitter is an 'open platform' meaning other people can develop tools (software and websites) which use the Twitter functionality and the published content (all the stuff that's displayed publicly on twitter.com, but not users' private messages or personal information). The API (application programming interface) is the publicly available information used by coders to do this. It enables sites like Tweetminster, Twittergrader and Hootsuite and applications like Tweetdeck to be created.

Risk Matrix

Criticism arising from an inability to meet the demands of Twitter users to join conversations / answer enquiries, due to resource and clearance issues.	Reduce by managing expectations with clear, published Twitter policy; use holding replies where answer will need research; (only if swamped) respond to 'themes'

	not individual replies.
Criticism arising from perceptions that our use of Twitter is out of keeping with the ethos of the platform (such as too formal / corporate, self-promoting or 'dry').	Reduce by sourcing varied content. Accept that there will be some criticism regardless.
Criticism of jumping on the bandwagon / waste of public money / lack of return on investment / pointless content.	Reduce by evaluating against objectives above and adhering to content principles.
Inappropriate content being published in error, such as: • News releases under embargo • Information about Ministerial whereabouts that could risk security • Protectively marked, commercially or politically sensitive information	Establish 'light' but effective procedural controls and guidelines for Twitter users; supported by communications professionals.
Technical security of the Twitter account and potential for hacking and vandalism of content.	Change Twitter password frequently using strong passwords; use cotweet.com to devolve access securely; avoid using unknown 3rd party tools that require the account password.
Lack of availability due to Twitter being over capacity.	Accept (affects all Twitter users, occurs rarely and brief). Take backup using tweetake.com and upload to Matrix every month.
Changes to the Twitter platform (to add or change features, or to charge users for accessing the service).	Review business case for continuing to use the service when any such changes are made.
Squatters / spoofers on Twitter.	Reduce by registering alternative names. Accept residual risk and

	monitor for this occurring. Report spoof accounts to Twitter for suspension.