TABLE OF CONTENTS

Background to the Social and Digital Media Policy .................. 3
Purpose of the policy............................................................... 3
  1. Principles........................................................................... 3
  2. Aims of the policy............................................................. 3
  3. Content and scope of the policy........................................ 3

Supporting framework and guidance................................. 4
  4. Legal framework.............................................................. 4
  5. Guidance.......................................................................... 4

Application of the policy................................................... 5
  6. What are social and digital media?.................................... 5
  7. Nottinghamshire Police’s use of social and digital media........ 5
  8. Social and digital media profiles – your information........... 6
  9. Standards of behaviour.................................................... 8

Policy review and monitoring............................................ 12
  10. Policy review................................................................. 12
  11. Monitoring...................................................................... 12
  12. Governance.................................................................... 12

Legislative compliance....................................................... 12

This policy, and associated guidance documents, has been developed and approved by the Chief Officer Team of Nottinghamshire Police to support the pilot project wherein a selected number of Neighbourhood Policing Teams use social media as a conduit for two way communications with their communities.

The pilot project will assess, among other things, the impact the application of this policy has on equality issues. Upon the completion of the pilot project, a full Equality Impact Assessment will be produced together with any other revisions required to this policy.

This is a small part of a wider communications strategy which will also examine and address equality of public access to communication channels.
Background to the policy

1. Purpose of the policy

The growing popularity of social and digital media as a means of communicating presents an opportunity for the force to enhance the way it engages with the communities it serves, both online and offline.

The use of such communication channels must be properly governed by the force in order to ensure they are used most effectively and to maintain and enhance its reputation and professionalism.

It has been noted by Her Majesty’s Inspectorate of Constabulary (HMIC: Without fear or favour, Dec 2011), that officers and staff would benefit from further guidance and clarification on the standards of behaviour expected of them when using social and digital media, both in a professional and personal capacity. It is intended that the guidance and training associated with this policy will achieve that.

2. Principles

Our use of social and digital media will at all times be professional, honest, transparent, accountable, ethical, appropriate, proportionate and justified in law. We will also be bound by the terms and conditions of use and codes of conduct set out by individual social and digital media websites and applications we choose to use, both in a professional and personal capacity.

3. Aims of the policy

- To provide officers and staff with an understanding of the standards of behaviour expected of them when using social and digital media, both in a professional and personal capacity.
- To establish arrangements for monitoring and governance of the use of social and digital media by officers and staff.
- To clarify the legal framework within which officers and staff must operate when using social and digital media on behalf of the force.

4. Content and scope of the policy

This policy is part of a wider Corporate Communication policy which includes the force’s policy on:

- Interaction with the media (press and broadcast media)
- Internal communication
- Stakeholder management
Supporting framework and guidance

5. Legal framework

Every interaction we have using social and digital media must be conducted within a legal framework to ensure that the public disclosure of information is lawful.

Those responsible for using social and digital media on behalf of the force must ensure all interactions comply with the website or application's terms and conditions of use and codes of conduct.

Numerous Acts of Parliament provide a context in which information will be disclosed to the public including, but not limited to, Contempt of Court Act, Magistrates Courts Act, Children and Young Person’s Act and the Sexual Offences Act.

In addition, the Data Protection Act, the Freedom of Information Act and Human Rights legislation further prescribe what information can lawfully be made public.

6. Guidance

In support of this policy, the following guides set out in detail and greater clarity for officers and staff how social and digital media should be used for professional purposes and what is acceptable behaviour online.

- Nottinghamshire Police: ‘Social and digital media guide – Engaging with the public’ (FOR INTERNAL USE ONLY)

The following guides give advice and guidance for officers and staff on using social and digital media sites securely for personal use, including recommended security settings.

- Nottinghamshire Police: ‘Using social and digital media securely – A guide for police officers and staff’ (FOR INTERNAL USE ONLY)
- Stop, Think, Connect: ‘Own Your Space – A Guide to Facebook Security’
- Get Safe Online: ‘The Rough Guide to Online Safety’
  http://www.getsafeonline.org/media/GetSafeOnline_RoughGuide.pdf

The following guide provides advice and guidance for officers and staff on using social and digital media sites for personal and professional use.

- Association of Chief Police Officers: ‘Guidelines on the safe use of the internet and social media by police officers and staff’ (see Appendix 1)
Application of the policy

7. What are social and digital media?

The terms social and digital media cover a range of online communication tools and services. These allow individuals and organisations to communicate and engage with each other online in a variety of ways. This includes:

- Social networking sites (ie. Facebook and Google+)
- Micro-blogging sites (ie. Twitter)
- Video sharing sites (ie. YouTube and Vimeo)
- Photo sharing sites (ie. Flickr)
- Audio sharing sites (ie. AudioBoo and Myspace)
- Online meeting platforms (ie. CoverItLive)
- Location-based networks (ie. FourSquare)
- Professional networking (ie. LinkedIn)
- Instant messaging services (ie. BBM, WhatsApp)
- Blogs (ie. Tumblr)
- Email/text messaging subscription services (ie. Neighbourhood Alert)
- Presentation sharing (ie. Slideshare)
- Forums
- Podcasts

8. Nottinghamshire Police’s use of social and digital media

The force’s social and digital media strategy is managed and directed by the Corporate Communication Department’s Public Engagement Team in order to support its priorities to cut crime and keep you safe, to spend your money wisely and to earn your trust and confidence.

The use of social and digital media by police officers and police staff, in a professional capacity on behalf of the force, is authorised by the Corporate Communication Department’s Public Engagement Team following consultation with other relevant colleagues, including the Force Information Security Officer and the Information and Communication Technology and Professional Standards Directorates.

The use of social and digital media by police officers and police staff in a professional capacity must be authorised in this way and ownership of the accounts is retained by the force at all times.
9. Social and digital media profiles – your information

YOUR PROFESSIONAL PUBLIC PROFILE (for example, an authorised force Twitter account)

Information acceptable on your professional public profile only

- Name
- Rank and collar number or job title
- Description of your role for Nottinghamshire Police
- Work location (provided you are not engaged in any covert activities or disclosing operationally sensitive details)
- Force contact telephone number (if you want it to be publicly available)
- Force email address or shared inbox email address (if you want it to be publicly available)
- Link to force website
- Photograph of yourself in uniform or smart work attire (against a blue or white background) or a force crest provided by Corporate Communication

Please see the Social and Digital Media Red, Amber and Green (RAG) Guide (Appendix 1 of the Social and Digital Media Guide: Engaging with the pubic) for information about what can and cannot be discussed when using social and digital media in a professional capacity on behalf of Nottinghamshire Police.

This information should not be published on your personal public profile unless otherwise stated in this guidance.

YOUR PERSONAL PUBLIC PROFILE (for example your personal Facebook profile)

Employment-related information

Nottinghamshire Police recommends that police officers and staff maintain separate professional and personal public profiles on social and digital media where possible.

Employment-related information acceptable on your personal public profile

- Name
- Reference to your job role in Nottinghamshire Police (provided it is not a covert role)
- Description of your role in Nottinghamshire Police (provided you are not engaged in any covert activities or disclosing operationally sensitive details).
- Reference to your work location (provided you are not engaged in any covert activities or disclosing operationally sensitive details).
- If you decide to make reference to your connection to Nottinghamshire Police on a personal public profile, you must include this disclaimer: “These views are my own and do not represent those of Nottinghamshire Police”.
Employment-related information unacceptable on your personal public profile

- Posting of restricted or higher information you have accessed in the course of your duties.
- Posting of operationally sensitive material that, if made publicly available, could jeopardise the effectiveness of a policing operation, or prejudice criminal, coronial or disciplinary proceedings.
- Posting or sharing of any material or links to any material that is defamatory against the force, another organisation or individual or that could bring the force into disrepute.
- Posting or sharing of any material or links to any material that could be deemed to be offensive, inappropriate or illegal.
- Publication of your force email address or telephone number.
- Images (still or moving) showing you at work, unless approved or previously released publicly by the force.

Please see the following guides for advice and information about protecting yourself when using social and digital media for personal use:

- Nottinghamshire Police: ‘Using social and digital media securely – A guide for police officers and staff’
- Stop, Think, Connect:: ‘Own Your Space – A Guide to Facebook Security’
- Get Safe Online: ‘The Rough Guide to Online Safety’
- Association of Chief Police Officers: ‘Guidelines on the safe use of the internet and social media by police officers and staff’ (see Appendix 1)

A note on Appendix 1 - Association of Chief Police Officers: ‘Guidelines on the safe use of the internet and social media by police officers and staff’ (see Appendix 1)

Section 8.2.4 of this guidance (page 8) outlines what information police officers and staff should not post on the internet and social media. Some of this information is permissible for officers and staff employed by Nottinghamshire Police to post on their profile should it be part of an authorised social media account used for the purposes of digital engagement on behalf of the force.

Section 5.3.1 of this guidance (page 6) recommends that police forces provide officers and staff with a method of communicating adverse comment or frustration in relation to organisational matters. Officers and staff are advised that the monthly online chat with the Chief Constable on the intranet and the comment facility on intranet news stories are provided for this purpose at this time.
Application of the policy

10. Standards of behaviour

YOUR PROFESSIONAL PUBLIC PROFILE

When using social and digital media on behalf of Nottinghamshire Police, officers and staff are expected to abide by the following standards of behaviour.

Act with honesty
Identify yourself as a police officer or police staff member on any accounts you hold for professional use and in any interaction with members of the public.

Treat others with respect, courtesy and fairness
Be respectful of those who interact with you and their opinions, but challenge if appropriate.

Act with integrity
Act according to the highest standards of professionalism, abide by police regulations and force policies, challenge unacceptable behaviour and report breaches to the relevant site if necessary.

Respect confidentiality
Only disclose information when legally allowed to do so and if necessary and proportionate (see RAG guide for further instruction).

YOUR PERSONAL PUBLIC PROFILE

When using social and digital media in a personal capacity, officers and staff will abide by the following standards of behaviour.

Identify yourself when discussing force-related issues
When discussing any issues relating to the force, it is expected that a police officer or police staff member will publicly disclose their relationship to the force, but make clear that their views and opinions do not represent those of the force. Police officers and police staff members are not expected to disclose details of their job role in their personal online interactions when not discussing force-related issues, but are reminded of their responsibility to maintain the highest standards of professionalism outside of work as well as in the course of their duties.

Anonymous interactions
When making any anonymous comments or postings on social and digital media, police officers and police staff members will not discuss force-related matters or disclose information gained in the course of their duties.

Disclosure of information
Police officers and police staff members are reminded that information gained in the course of their duties should not be disclosed outside of the force otherwise than in accordance with their duties.
Application of the policy

Privacy and security settings
Police officers and police staff members are issued with guidance on recommended privacy and security settings for social and digital media accounts for personal use. They are advised to follow these recommendations in order that their privacy and account security is protected.

Use of force systems
The use of force computers to access social and digital media for personal use is prohibited. See the force’s Internet Usage Policy for more information.

Disciplinary action will be taken against any police officer or police staff member who deliberately makes improper use of social and digital media.

What the public can expect from us and what we expect from the public
(these guidelines are published on the force website)

Nottinghamshire Police uses social and digital media to communicate with the public and enhance the way we have conversations with the people we serve.

We use several platforms to achieve this, including Twitter, Facebook, YouTube, AudioBoo and CoverItLive. For a complete list, visit www.nottinghamshire.police.uk/contact

Content, such as appeals for information, images of suspects, missing person appeals, daily news items, images, video and audio, are posted on these sites. We do this for a variety of reasons - to seek your help in fighting crime, to raise awareness of issues that could affect you and to keep you informed of news from the force.

Every day we are communicating with around 30,000 people using social and digital media and we encourage you to communicate with us using these channels.

What we expect from you

1. Never use social and digital media channels to report a crime or information about criminal activity to us. Please call us on 999 in an emergency or 101 when it’s less urgent to report a crime. You can also call Crimestoppers on 0800 555 111 to report information about criminal activity.
2. Do not post messages or content that could be deemed to be:
   - Abusive
   - Defamatory
   - Racially offensive
   - Sexually offensive
   - Obscene
   - Inflammatory
   - Unlawful
3. We want everyone to feel comfortable using our sites to communicate with us so please do not swear in your posts or post anything distasteful.

4. Do not use our sites for posting spam or adverts for products or services you or your business offers.

5. Do not post your personal details, such as your address or phone number, when posting publicly on our sites. If you have contacted us and an officer or staff member wants to contact you in return offline, they will privately message you, if possible, asking for your contact details. Only provide these if you are comfortable doing so.

6. Do not post any material that you do not own the copyright to.

7. Do not pretend to be someone else.

We reserve the right to remove posts or block any users that breach these guidelines, without explanation.

What you can expect from us

How often will I see your updates?

If you follow us on Twitter or ‘Like’ us on Facebook, you can expect to see several updates daily – more frequently on weekdays, but also at weekends.

If there is a major incident that affects a lot of people in Nottinghamshire, or an emergency situation where getting accurate information and instructions to you quickly is essential, we will use Twitter as the main platform for distributing that information. Much of the information will contain links back to the force website for a more detailed explanation.

Will you reply to me?

If you send a tweet to us or post on our Facebook page, you can expect a response, if required and appropriate, but we cannot reply to everyone who posts to us and it may not always be possible to reply immediately. When we are not going to be able to monitor our Twitter and Facebook accounts for a considerable amount of time (for example, over the weekend) we will endeavour to let you know, explaining when we will be back online.

There are some topics or cases that we will not be able to discuss due to a number of reasons, including criminal proceedings being active or investigations being under way. If this is the case, we will tell you.

Can I report crime online?

At this time, we cannot take reports of emergencies or crime over social and digital media platforms. That is not because we don’t take these reports seriously, but because we do not have sufficient resources to provide a 24/7 service in this respect. If you try to report a crime in this way, you will be asked to contact us by telephone or visit a police station to make a report. In an emergency, you should always call 999.
Can I follow my local beat team?

Our plans for extending our use of social and digital media in 2012 include enabling more police officers and staff members across the force to use communications platforms, including Twitter and online meetings, to engage with you. Keep an eye on our Twitter account and website for announcements when officers arrive online.

Why are you following me?

If we follow you on Twitter, please don’t assume we are monitoring your online activities or you are in trouble. We follow people and organisations that we are interested in and relevant to policing, community safety, Nottingham and Nottinghamshire in general.

What you can expect from us

Do you remove posts?

Generally, we will not remove posts from members of the public that are made on our social and digital media channels, as we really want to hear your opinions on the issues that matter to you and have a conversation with you, while maintaining a family friendly format.
However, we will consider removing posts or blocking users or accounts that breach the guidelines outlined above, without any explanation.

Did you know?

You don’t have to be signed up to Twitter to follow us. If you have internet access, you can visit www.twitter.com/nottspolice to see all of our tweets. If you do not have internet access, but have a mobile phone, you can ask for our tweets to be sent by text to you using Twitter’s Fast Follow service.

To sign up to the free service, text Follow nottspolice to 86444 (on Vodafone, Orange, 3 and O2).

You will start receiving our tweets by text to your mobile phone every time we post a tweet.

To stop the messages, text STOP or OFF or LEAVE to 86444.
Policy review and monitoring

11. Policy review

This policy will be reviewed annually, by the Head of Corporate Communication in liaison with the Deputy Chief Constable and approved and adopted thereafter by the Force Executive Board.

12. Monitoring

Corporate Communication staff responsible for the force’s use of social and digital media are also responsible for monitoring the use of social and digital media for professional purposes, by police officers and police staff members in order to protect the Force’s reputation. In addition, their role is to train, advise and guide those tasked with digital engagement.

Monitoring of social and digital media use by police officers and police staff members for personal use is undertaken by the Professional Standards Department.

13. Governance

The Corporate Communication Department is responsible to the Deputy Chief Constable for the governance and review of this policy. Specific responsibility rests with the New Media Communications Officers and the Public Engagement Manager.

LEGISLATIVE COMPLIANCE