Lincolnshire Police
Social Media User Guidance

Definitions
Social media is a term used to describe the type of media that is based on conversation and interaction between people online through the sharing of information, opinions, knowledge and interests. Where media means digital words, sounds and pictures which are typically shared via the internet and the value can be cultural, societal or even financial.

Source: Wikipedia.

For the purposes of this guidance 'social media' refers to all online engagement platforms used to facilitate two way conversations, both internally and externally and, as the name implies, involves the building of communities or networks, encouraging participation and engagement. This includes, but is not limited to Facebook, Twitter, Yammer, Bebo, You Tube, MySpace, Blogs, internet forums and chatrooms and feedback pages on local media sites.

This guidance and the associated policy on social networking and video sharing websites should be followed at all times when a member of Lincolnshire Police uses any form of social media in an official capacity, or where the public might assume that such use is in an official capacity.

Summary
In summary these guidelines cover the following points:

- All official online communication must be **authorised**. This is through line managers and the Digital Media Working Group via the force Website Officer or Marketing Manager at force headquarters

- Staff making official use of online media should **disclose** their position and status and the fact that they are authorised to communicate an official viewpoint

- Staff must be aware of and comply with laws and policies for the appropriate protection of **official information**

- While staff should be receptive to ideas and comments provided online by stakeholders, they themselves should avoid any statement that could be **perceived as criticising force policies**

- Information and views provided should be **accurate, clear** and expressed in such a way that it cannot be misrepresented

- All communication should be **professional, courteous and constructive**

- Systems should be in place to ensure that online communication is **consistent**, with information and advice being provided by the force through other media and forums

- Intellectual property, copyright and privacy issues need to be taken into account and advice sought if there is any doubt.

Use and Purpose
The innovative world of online communication is evolving constantly and Lincolnshire Police must evolve with it to communicate more effectively with members of our communities. Sites such as Facebook give the opportunity to engage with a much

wider group of people in addition to those reached through traditional methods, allowing anonymous or more discrete contact with the police from users who might not engage through traditional channels.

Before starting up a social media platform, be aware of what you expect to achieve, and how this links to force, departmental and / or neighbourhood priorities.

All official communication platforms will use common branding in order to prevent confusion for users and this will be provided on a template by the force Website Officer. Remember it is easy for others to set up malicious copies of Facebook profiles etc, so the force will arrange for verified accounts and ensure that corporate branding is used.

The content should be professional and appropriate to your audience. Simply issuing 'press release' style updates will fail to engage most users, and you should be prepared to have a conversation with the people who post, in much the same way as you would in face to face situations. Engaging through social media is another way of striking up a conversation; if you're not prepared to have that conversation, don't start it.

The exact nature of the content you post is up to you. As long as it complies with the law, addresses the priorities of the force, department and / or neighbourhood, and is not sensitive, then you should feel free to use the opportunities presented by social media to address these priorities. Some good examples of how Facebook and Twitter have been used in policing can be found in North Yorkshire Police and West Midlands Police – the Digital Media Working Group can provide more details.

Above all, don't just be on Facebook and Twitter because everyone else is on Facebook and Twitter. Know what you're doing there, understand how this links into your priorities and those of the force and have a plan to make this part of day to day business.

See Appendix A for examples of useful content.

Control, Access and Authorisation
Remember that what you post is public and difficult if not impossible to remove. Lincolnshire Police expects high standards of all police officers and staff and this includes when using online communication. The simple rule is not to post anything that you wouldn't want to see repeated on the evening news.

Remember that copyright laws apply so any video, audio and pictures used must have the copyright owner's permission. If in doubt ask the force Website Officer or Marketing Manager before posting.

Remember that information that could compromise an ongoing investigation or reveal confidential or restricted information should never be posted online. Treat online communications in the same way as you would public meetings and consider what information is used **carefully**.

Remember that online it is much easier for people to connect several seemingly unrelated pieces of information. Ensure that everything you post is thought through carefully to avoid unintentionally revealing sensitive information.

Be careful about identifying individuals directly or indirectly. Data protection still applies and ideally permission should be sought from those who appear in

photographs or videos. This is particularly true when the subjects of such media are children. If in doubt ask the Marketing Manager before posting anything. It is strongly recommended that hard copies of any such permissions are retained.

See Appendix B for detailed guidance on photographs and video.

Access to social media sites to post should be actively managed by the poster's line manager. Abuse or inappropriate use will be dealt with through normal disciplinary procedures.

Use of intelligence gathered through social media sites is covered in Appendix C.

Information regarding risks is detailed in Appendix D.

The personal use of social media is covered in Appendix F.

Don't…

- Be afraid to challenge other people's inappropriate language. Police sites will appeal to all ages and all members of the community and as such offensive language from users is not acceptable

- Delete critical comments as long as the language is appropriate for younger users. Address each comment as quickly as possible and with the utmost professional tone. In the case where someone just can't be satisfied or reasoned with, do not continue in a back and forth debate, which almost always ends in a negative and unprofessional way and consider removing the comments. See Appendix E on Security Operating Procedures for more guidance

- Assume that people online are who they purport to be. Masquerading as other people is common online, both for fun and for more malicious purposes

- Start an online presence, simply to let it fade away. This is as much as part of community engagement as other neighbourhood policing activities and should only be started if appropriate resources are available to manage it

- Be afraid to recognise and acknowledge mistakes in posts, subject to legal constraints. If a factual error has been made, correct it in such a way that the correction is obvious and doesn't simply 'cover up' the error

- See online engagement as a replacement for face to face policing. This is simply another way to reach our communities and should be used alongside more traditional engagement methods

- Use nicknames, slang or police jargon. This may lead to misunderstanding and exclude people who do not understand.

Do…

- Be ready to converse with anyone who contacts you. Be accessible, appear interesting, approachable and human and be willing to engage. Remember this is a two way conversation, not a one way passing of information

- Build a relationship with users. Where appropriate use the 'follow' or 'like' functions to follow other users in order to build relationships – but explain why you are following people so it doesn't appear like Big Brother

- Publicise your online presence through business cards, posters etc., alongside phone numbers and email addresses

- Be responsible for what you write. Free speech is great, but it doesn't mean you are free to say what you wish. Remember you represent Lincolnshire Police and we trust you to do that with PRIDE

- Use this as a tool to assist policing. Social media can be a source of intelligence, target hardening and increased detections as well as improving engagement. Social media is not a separate thing from normal policing and should not be treated as such. See further information regarding intelligence at Appendix C

- Ensure that where accounts are shared (for example across a neighbourhood policing team) that arrangements are in place to allow access to the site for when key people are on leave or other wise abstracted. Nothing is worse than providing a facility for conversation, and then not replying to questions

- Make clear how comments and queries will be dealt with – for example emergencies should always be directed to 999. Be clear about how quickly people can expect a reply to other issues – and stick to this

- Be interesting and informative, and interested in other's comments

- Personalise comments (e.g. 'xxxx neighbourhood team asks…' 'I need help with…'. Use pictures of the team and area, rather than stock photos. Appendix B has more guidance on photographs and video

- Protect your personal privacy and that of others by not including personal information of either yourself or of others in your posts (such as names, email addresses, private addresses or phone numbers)

- Have links back to the Lincolnshire Police main website and any other relevant local sites (e.g. other neighbourhood policing teams nearby)

- Engage people in conversations where they are happening. You represent Lincolnshire Police and we trust you. Act accordingly

- Give people not just information, but the power to choose how they want their problem resolved

- Ask for guidance and support – available from the Digital Media Working Group or via the force Website Officer

Appendices:

Appendix A – Ideas for Content
Appendix B – Photographs and Video
Appendix C – Intelligence
Appendix D – Risks
Appendix E – Security Operating Procedures
Appendix F – Private use of online media.

DMWG/V3
September 2010

IDEAS FOR CONTENT

Below are some generic ideas for content. The approach is not necessarily to use all of these all the time, rather to use the appropriate approach for your area and for your users.

1. **Profile** Each Facebook page has a profile box. When this is updated all those who have joined our Facebook page will see the change when they log on to their own Facebook page.

    The profile box starts off with the text i.e.:- *Carholme NPT is……..* We can then add relevant information afterwards ie, *holding a patchwalk today on Carholme Road at 1800hrs.*

2. **Priority Survey** Link your page to the force website and Facebook page in order to access things such as priority surveys. We need to take advantage of every opportunity to distribute these surveys and this again is another great platform for this.

3. **Events/Engagements** Promote the events happening in the local area, e.g., targeted foot patrols, meetings, and crime reduction events. This should be updated regularly with anything we are involved with that people will be interested in.

4. **E-mail** Facebook allows customers to contact us via email. Encourage this to give more complex information, ask questions, and receive intelligence.

5. **Video** Facebook allows us to post videos on our page. We would like video appeals for information, CCTV, training of dogs, warrant videos and event videos. Posting videos, information appeals and CCTV clips gives us further opportunities to reach a wider range of the public. All video footage is produced in-house by the force TV unit within Corporate Communications. If you wish to post any video footage contact the force Website Officer or the force TV unit.

    Training and warrant videos give the public something back from the police. It allows them into places they would not normally get access. Snippets from behind the scenes gives an insight into all the training and hard work we do.

    Event videos allow our customers to see what activities we are getting involved with in the local area - attending the local youth club, diversionary activity or local summer fair for example.

    Use of video and photographs will make you and the force more approachable and more human.

6. **Pictures** We would like pictures on Facebook for much the same reasons as videos. Visuals are far more likely to grab the attention than text. Areas for consideration could be pictures of wanted persons, missing persons, stills from CCTV, events attended, again the possibilities are endless.

7. **Wanted Appeals** We would like to post information of persons wanted in our area, with links back to the main force website for text, pictures and videos. The appeals need to be timely and relevant and linking back to the main website ensures this happens. For further advice on posting appeals, contact HQ Press Office, or the Website Officer.

8. **Missing Appeals** As per wanted appeals.

9. **Contact details** It is essential to have all contact details on the Facebook page, including e-mail addresses, contact numbers (work issued mobile numbers, 0300 111 0300 and emergency), station opening times, beat priorities etc. Include details of how quickly people can expect a response from these communication methods.

10. **Blogs** Blogs are 'day in the life' prose to be created by any individual officer to aid the public to better understand the police and the different roles in the policing service. In general they should be interesting, concise, informative accounts with positive information, and have a personalised manner – giving the reader an insight of being with the officer in question.

    They must not show any political allegiance but need to demonstrate the neutrality of a modern police force.

11. **Links** Facebook pages should link to the following or similar information, promoting our partnership and crime reduction work:

    *   **Neighbourhood Watch**
    *   **Crimestoppers**
    *   **Partners such as Lincolnshire County Council, borough, town and district councils**
    *   **Ringmaster**
    *   **Lincolnshire Police Website**
    *   **Immobilise.com**

12. **Operations and Initiatives** We would like to provide customers information about operations and initiatives we have launched or are underway. This should reflect force and local priorities, and explain what we along with our partners are doing to address local issues affecting local communities.

13. **On-line surgeries** The force is looking into technologies that will allow beat surgeries and other public meetings to be held on-line. This has been trialled in other forces and has been a great success.

14. **FAQ (frequently asked questions)** Numerous people often ask the same questions. In light of this, we felt that a pre-emptive frequently asked questions information board would be time saving and informative.

    For example, if the customer has a question regarding nuisance neighbours, we can post links, advice and information on what police and partners can do to help with their problem.

PHOTOGRAPHS AND VIDEO

Photographs and Video fall into three categories A, B and C depending on the content. The category will inform who can authorise their use on the site and under what regulation.

Category C will be photographic or video images containing police personnel only. These images will have been taken with consent for this purpose or with acknowledgement.

Category B will contain images or video of public events, or have been taken in public spaces. Category B will also include any image involving in part or whole persons other than police staff. Permission for use for this purpose must be gained from the persons involved OR from an appropriate adult (as is appropriate to the case).

Category A will contain images or video that could be defined as any of the following.

- APPEALS
- MISPER
- INCIDENT RELATED (such as drugs seizure)
- CAMPAIGN RELATED (such as seat belt use, mobile phone, drink drive)

All photographs and video will require appropriate line management approval for use. Professional integrity of the force must be maintained and images should reflect a quality and standard in line with force guidelines. No damaging, inappropriate, lewd or offensive images must ever be displayed using this media.

This media is open to all age groups and this is to be borne in mind when uploading images, especially those falling under Category A.

INTELLIGENCE

Members of the public can become friends or follow a police online presence. There is an implied permission that personal profiles can be viewed upon accepting to be a friend or fan. This gives a community intelligence tool which must be properly managed.

Despite implied permission, no intelligence will be gained from these profiles without agreement from an appropriate supervisor. Upon this agreement the authorisation of the BCU Commander must be obtained with a direct authorisation for the use of this method and the limits to the information sought.

Using those who have chosen to follow Lincolnshire Police to gather information about one of *their* friends or contacts who has not themselves befriended Lincolnshire Police is **NEVER** appropriate.

ALL OFFICERS MUST BE AWARE OF RIPA - all persons involved must be aware of RIPA and its effects. Intelligence gathering under any circumstances must be informed by this legislation.

The email facility gives a relatively anonymous way to deliver information to Lincolnshire Police. There is the potential for new intelligence to be passed via this method of engagement as it encourages persons to support the local police. This is to be managed according to existing procedures and policies.

Where information is of such quality or importance or where a source continually provides information then the source of this information will be put forward as appropriate as a source – CHIS, in line with standard force procedures for this, working closely with the DIU in relation to any internet sources of information and taking guidance for any referrals from such sources of intelligence.

The force policy **MUST ALWAYS** be adhered to with reference to CHIS.

At all times information must be treated as confidential. All efforts must be taken to ensure the identity of persons providing intelligence remains confidential.

RISKS

The use of social media is not without risk. Much of the risks are similar to those present in other forms of public engagement. There are however some differences, most notably around the permanence and accessibility of information posted. The primary risks identified are:

1. That a member, or members, of the community will suffer harm or distress as a direct or indirect consequence of information posted onto a force Facebook profile by a member of the force or a member of the public.

2. That the force will suffer negative publicity, loss of public confidence, and/or potential financial penalties arising from damaging information posted onto a force Facebook page by a member of the force or a member of the public.

   Facebook and other social media websites are widely used by younger individuals who may have a limited perception of the risk that posting personal information about themselves or others might pose. There are recorded instances of young individuals suffering harm (including suicide) as a consequence of information that has been posted about them, either by themselves or by others (the latter, frequently in the form of 'cyber-bullying').

   Conversations that take place on such sites descend, with relative frequency, into arguments including racist or homophobic comments and other offensive remarks. Whilst the force's use of Facebook represents a potentially effective method of engaging with the local community that it serves, it must always be remembered that Facebook has world-wide access and the risks of misuse or inappropriately posted information are increased accordingly.

Mitigation of Risk
Information will be posted by representatives of the force to its Facebook pages and other social media sites. There will be the opportunity for members of the public to post comments, and for a conversation to take place. The two risk types identified above can be significantly mitigated by:

1. A highly visible and clearly worded warning to users not to post personal information or other sensitive information onto the site and guidance on how to appropriately report crimes or discuss sensitive matters directly with the Force.

2. A disclaimer that states that comments posted by members of the public to Facebook do not necessarily represent the views of Lincolnshire Police.

3. Significant care, by force representatives, to post no information that potentially identifies members of the public, other than where there is a policing necessity and where appropriate authorisation has been given in accordance with UK legislation. It is very strongly recommended that wanted or missing persons are not referred to unless there is an associated appeal for public information on the force website. In this case, the Facebook details should be minimal, e.g. '*Can you help find nine year old Susan Smith? For details please click here* (link to appropriate page of force website)'. This

approach will minimise the risk that personal details are disclosed inappropriately and will help ensure that the information relating to the missing/wanted person is updated dynamically and accurately.

4. An expectation that individuals who post information to Facebook on behalf of the force adhere to the conditions and constraints prescribed in this document and other force polices at all times. Individuals should be fully briefed on these requirements and that their ability to post information appropriately is assessed by a line manager before they are provided with access to Facebook.

5. At least daily checks on information posted on the force's Facebook pages, with appropriate response action taken – this will include the immediate removal of inappropriate postings.

6. Operational ownership of the use of social media sites, with owner responsibilities to include:

   a. Defining clear and measurable ways of determining the level of success of the use of social media;
   b. Dynamic management of the use of such sites, ensuring that appropriate remedial action is taken if it is found to pose unacceptable risks;
   c. Overall responsibility for the standard, appropriateness and timeliness of information posted to, and removed from social media sites by the force;

Subject to technological issues, it is proposed that on-line surgeries are held, representing a 'live' discussion between a Lincolnshire Police representative and members of the public. Whilst it is hoped that most members of the public would use this facility constructively, there is a more significant risk that this facility would be utilised by those individuals seeking to cause harm to the force or to other Facebook users. Provision of a system allowing some form of 'pre moderation' of user comments is strongly recommended.

SECURITY OPERATING PROCEDURES

In addition to the requirements outlined in the main body of this document, the following procedures must be adhered to.

Line managers will:

1. Ensure that all force representatives who have write/modify access to the force Facebook pages are made aware of their responsibilities and are able to submit information to Facebook professionally and appropriately.

2. Address risks associated with social media appropriately and expeditiously.

3. Ensure that the benefits and risks are measurable and that the appropriate data is collated, analysed and used to make decisions regarding the value of using social media.

4. Ensure that a warning and disclaimer is clearly visible on all pages to which information may be posted by the public. This might state, for example: **'Whilst Lincolnshire Police welcomes your views, comments and questions, it does not wish to put you, or anyone else at risk of harm. If you need to report a crime anonymously, please telephone Crimestoppers on 0800 555111. If you need to contact Lincolnshire Police about a crime or incident, or discuss something with us in person, please click (hyperlink) for our contact details. Please note that any views posted by members of the public on these pages do not necessarily represent the views of Lincolnshire Police'.**

5. Ensure that all pages on which public postings can be made are checked at least daily, and that identified issues are addressed, including the rapid removal of inappropriate material.

Force Representatives with write, modify or delete access to the Force's Facebook pages will:

1. Adhere to the standard operating procedures of this document.

2. Avoid naming individuals, other than where expressly permitted by this guidance.

3. Only name wanted or missing persons, where a public appeal already appears on the force website. Details recorded on Facebook regarding such persons should be minimal, and a hyperlink should be created to the relevant page of the force website.

4. Discourage members of the public from identifying themselves or others, or providing intelligence or other sensitive information on the Facebook page.

5. Check information posted to the pages with the frequency directed by line management (these pages should be checked at least daily, and it is assumed that this will be a shared responsibility) and take action appropriately. This includes the removal of inappropriate material, including postings that:

    a. Identify a living individual;

b. Include intelligence or other sensitive material (ensuring that this is first fully recorded with time and date, and referred or dealt with appropriately);

c. Contain content that is likely to offend – this will require a degree of judgement. It may be deemed appropriate to retain comments that use strong language as a means of expression, in the interests of free speech. However, comments directed at or likely to offend a specific individual or group (e.g. racist, homophobic remarks or personal insults) should always be removed.

PRIVATE USE OF ONLINE MEDIA

In relation to the private use by police officers and staff of online communication, the fundamental principle is that this should not be done in work time using force resources. Private blogging or other online communication at work is not permitted and staff and officers who blog from work can be identified easily by their email addresses.

There may be cases where it is appropriate for staff and officers to communicate online with issues that may not be directly work related but are important to the maintenance of individual knowledge and capability. Managers who believe that this is an appropriate private use of online communication resources should have guidelines in place to cover these situations.

Officers and staff who blog in their own time using their own resources are covered by the same broad principles that apply to comments in a private capacity on public issues. Staff and officers are entitled as private citizens to do so, but they must avoid comment that might be interpreted as an official statement on behalf of the force or that compromises perceptions of their ability to do his/her job in an unbiased or professional manner.

It is strongly recommended that individuals consider how easily members of the public or the media could link private and force postings to identify individuals and cause distress or embarrassment to both the force and individual.

Where staff and officers wish to use social media sites outside of work they should consider the use of a disclaimer along the lines of **"Opinions, links and content are my own personal views and not the views of Lincolnshire Police"**. Officially sanctioned social media presences should not be used for purposes outside of those agreed for work.