Social media handbook for law enforcement to support cybercrime prevention and awareness

Version 1A
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2. What are social media?</td>
<td>4</td>
</tr>
<tr>
<td>3. Social media value for law enforcement</td>
<td>5</td>
</tr>
<tr>
<td>4. How to use social media for prevention and awareness purposes?</td>
<td>6</td>
</tr>
<tr>
<td>4.1. Goals</td>
<td>6</td>
</tr>
<tr>
<td>4.2. The social media &quot;check-list&quot;</td>
<td>7</td>
</tr>
<tr>
<td>4.3. The social media road</td>
<td>9</td>
</tr>
<tr>
<td>5. Best practices</td>
<td>10</td>
</tr>
<tr>
<td>6. Conclusions</td>
<td>11</td>
</tr>
<tr>
<td>7. Useful links</td>
<td>11</td>
</tr>
<tr>
<td>8. ANNEX: About the law enforcement practitioners cooperating on this</td>
<td>12</td>
</tr>
<tr>
<td>Handbook</td>
<td></td>
</tr>
</tbody>
</table>
1. Introduction

Over the years, Internet has evolved from static web pages, where users simply read or downloaded content, towards a new online concept (aka Web 2.0), characterized by greater user content generated technology, global network connectivity and enhanced communication channels.

The social nature of Web 2.0 is one of its strongest components. Increasingly, websites enable community-based and user-generated input, interaction, content-sharing and collaboration. Anywhere, at any time, just by connecting an electronic device to the Internet.

The potential of this innovation has not passed unnoticed by business, citizens and criminals alike. With more than 3 billion Internet users in the world and the speed with which technology brings new developments to the market, anyone connected can become a victim of cybercrime. In this context and due to the characteristics that we will explain more in detail later, social media offer to law enforcement a unique set of communication channels.

As a consequence, within the 2015 Operational Action Plan (OAP) of the EMPACT Priority G Cybercrime Attacks, the Strategic goal 7 has been set up "to strengthen cyber security awareness, responsibility, resilience and agility of private users and professionals, in particular operators of critical infrastructure and information systems, in order to minimise threats to victims and damages of cybercrime". This Strategic goal is to be achieved at least partially through the elaboration and distribution of a Handbook for the use of social media in support of law enforcement, particularly to advice police forces on how to make more and better use of these tools for prevention, awareness and communication of cybercrime threats and trends (from now on called "Handbook").

This Handbook could also support those law enforcement agencies looking to develop and exploit the potential of social media engagement or assist those without social media implemented yet on preparing the business case for the integration within their national communication strategies, providing them with an overview of potential values, goals, resources needed and benefits to obtain from the cybercrime prevention and awareness point of view. It is up to each Member State to individually scan its national situation and tailor the social media implementation accordingly.

It is outside of the scope of this exercise to create a dedicated product for the use of social media in general, although basic references will necessarily be made; or a social media policy outlining for police officers the corporate guidelines or principles of communicating in the online world. It is also not intended to cover the use of social media as investigative tool for law enforcement to solve and prevent traditional crimes.

This Handbook has been drafted in consultation with a small number of practitioners from those countries that have successfully introduced and implemented new information and communication technologies to improve the police relationship with the public, especially by means of engagement, and to

---

1. www.internetlivestats.com
Europol Public Information

transmit prevent and protect messages in a swift and cost efficient manner. Specific reference to them is done in the Annex at the end of this document.

2. **What are social media?**

While in theory social media can be defined\(^2\) as websites and applications that enable users to **create and share** content or to participate in **social networking**, in practice, the concept of social media is very broad and its characteristics very dependent on the specific community that uses each particular channel.

Nevertheless, there are a number of **benefits** likely to emerge when using social media:

- **SPEED:** immediate end-user reach;
- **POWERFUL PROPAGATION:** which allows viral and massive reach due to its broadly extended use, especially with the mobile device use expansion;
- **INTERACTIVITY:** a two-way engagement which allows the creation and development of virtual communities;
- **LOW COST:** technology and platforms can be used free of charge; however, their correct use and management require human resources and time in order to achieve results;
- **SCALABILITY:** easy to tailor to the user’s needs;
- **FLEXIBILITY:** technology in constant evolution;
- **COMPLEMENTARITY:** social media messages can be strengthened by combining them with traditional means of communication, e.g. broadcasting news.

Risk to take into account: users worldwide are getting accustomed to incorporate social media as part of their lives. The familiarity with the existing tools can develop the social perception of trust towards new or similar platforms, making the user too relaxed in terms of security and risks awareness.

There are many different platforms available on the market, with different characteristics, functionalities and targeting different user demographics. Often, users of one social media platform will not use the others as regularly. Also, even the same platform will not be used for the same purposes by its users.

The following channels have been picked only as an **example** of the currently most broadly extended:

- Social networking sites: i.e. Facebook
- Business and professional networking sites: i.e. LinkedIn

\(^2\) [http://www.oxforddictionaries.com](http://www.oxforddictionaries.com)
Europol Public Information

- Micro blogging: i.e. Twitter
- Video-sharing sites: i.e. YouTube
- Photo-sharing sites: i.e. Instagram, Flickr
- Instant messaging: i.e. Whatsapp, Viber, Skype

As the practice evolves, they are also taking characteristics from each other. For instance, Facebook is being increasingly used for video sharing and engagement over YouTube; or the level of social networking in Instagram in higher than in Flickr, even if both are photo-based channels.

Others: forums, blogs, wikis, websites and online dating sites are to be considered as social media platforms as well.

3. **Social media value for law enforcement**

In the digital age, law enforcement can and should when possible benefit from the social media characteristics mentioned in the previous chapter. This can be done by integrating social media as part of the national/regional/local communication and community engagement strategies. Social media can help police to become valuable for the community in terms of cybercrime prevention and awareness, and once this is achieved, to become influential.

Law enforcement could use social media for the following general purposes:

**PERCEPTION:**

- To show to the public a different police side, not only more human but also more useful, explaining what services can law enforcement provide to the community;

**COMMUNICATION AND ENGAGEMENT:**

- To reach out to the community: by engaging with individuals (who otherwise would not be reached) and by sharing information (otherwise not covered by traditional outlets);
- To release timely/reliable information, before, during and after any given event or situation; (directly related to the next point)
- To address the community concerns: by promoting engagement rather than broadcasting, by listening to their voice and answering in return to keep the community safe and reassured;
- To share alerts and warnings and explain how to better protect devices.
INVESTIGATION:

- To help to solve crimes (to a certain extent): a lot of information can be received via this channel directly from the public;

- To promote “self-help”: informing the public what to report to the police and how to secure helpful evidence to support a police investigation. Also where to go if it is not a police matter (for instance, directly to the social media channel provider).

4. How to use social media for prevention and awareness purposes?

The main challenge for law enforcement is to influence the public perception towards cybercrime and to reduce the fear, making the community more resilient and ready.

Whether a law enforcement agency would like to begin using social media or the channel is already up and running, the following chapters are meant to either help with the start-up assessment or to improve/enhance the existing activities.

4.1. Goals

Police pages and profiles are to become the most trust worthy source of information in cyber security, since they are the source that most likely the public will turn to when they are affected by an incident.

<table>
<thead>
<tr>
<th>What are the specific goals that can be achieved with social media in the area of cybercrime prevention and awareness?</th>
<th>How can those goals be achieved?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>by defining and explaining what is cybercrime, so the public can understand the dangers, using their own language and targeting different audiences depending on the message.</td>
</tr>
<tr>
<td>Protection</td>
<td>by empowering the audience, making them acquainted with the risks and giving them basic knowledge to avoid becoming a victim.</td>
</tr>
</tbody>
</table>
| Awareness | by communicating existing cybercrime threats and trends, as well as new ones as they occur, and warnings.  
*Community involvement/collective intelligence:* the public can share real and current cases with the police (i.e. scams, phishing emails). The police can then use this information to warn the whole community or dispel rumours. |
### Prevention
by targeting potential cybercriminals, especially young people, pointing out the severe legal consequences of committing cybercrime and promoting lawful alternatives for the use of computer skills (i.e. cybersecurity).

### Reaction
by constantly reminding what to do in the event they become a victim, indicating where and how to report the incident and what to do if an electronic device has been infected.

### Information
by sharing links to national resources (i.e. police websites, private sector partners, red lines, child protection, etc.)
by reinforcing the messages combining police social media content with media in general, for instance when communicating the results of operations against cybercrime, seizing the opportunity to work on any of the previous five goals described.

### 4.2. The social media “check-list”
Before starting any law enforcement social media account(s) it is important to make an initial assessment of the amount of resources (infrastructure, staff, time and budget) that will be required to successfully implement and manage the channel(s).

#### The team

**Location:** Typically, the social media team will be part of the broader police communications/press office team, whether national, regional or local.

It is up to each country to determine the number of channels and the area of action, as well as the specific number of staff allocated to social media in each case. It is generally considered that the message reaches better the end user when delivered by the local police, or by an authority as close to the target as possible.

**Composition:** It will always be important to have on the team a combination of at least one person (police officer or not) with a sound background on Communication, as well as law enforcement members, to understand the legal and operational implications of the incidents and to be able to answer questions in a professional and accurate manner.
While there may not be an explicit need to create a specific group to communicate exclusively on cybercrime matters, the social media team is to be closely linked to the (cyber) investigators, creating a fluent flow passing on the information received from the public, obtaining swift answer to more technical and legal questions related to police matters and making sure that no message is sent out which could jeopardize on-going investigations.

Training: Social media and community management training is recommended and considered as key. It could also include a combination of daily practice (where the officer will learn to detect relevant content, its urgency, the need or not to react or to follow up with the investigators, etc.) with theory and best practices passed on to each new member of the team.

It can take some time for the new officer or police staff member to develop the necessary aptitudes and communication skills. While some teams will choose a very small group dealing with the account management, others will prefer training more officers and using existing software available in the market to monitor who is doing what and avoid duplication.

Account and content management

- The same social media team is advised to manage all the channels under its domain, seeking for vertical collaboration among communication teams (national – regional – local) when needed.

- Whether there are many or just a few officers with social media accounts (with the possibility to react by posting, commenting and replying), it is common practice that only a small number of people will be responsible to decide on content and campaigns, in order to ensure message consistency and tone.

- The content management of the channel shall be a combination of yearly forward planning and daily reaction to trending topics, newly identified threats and trends and general news, seizing opportunities supported by the key high-impact coordinated dates that relate to police activities, awareness campaigns and operational activities, always aiming at achieving the goals described under chapter 4.1.

Budget

- A social media channel could be run with zero extra budget.

- However, the staff allocated may require specific training and additional expenses may be needed to be online 24/7 or monitoring as many hours as possible. Also, there is a need to have implemented the infrastructure to allow the secure access to the platform(s). All this may occur on extra charges.
• If possible, it would be worth having a flexible small amount of budget allocated, to help some messages get through more easily, for instance, to place police announcements as advertisements in specific pages used by the community that needs to be reached.

Policies and procedures

• Drafting a general Communication Strategy for the national/regional or local police would be very beneficial to guide the social media activities, since they need to fit within the global picture and follow the same mission and values.

• Depending on the size of the social media team and the channels managed, it would be advised to further describe in procedures the division of roles and responsibilities and the daily management of the account(s).

4.3. The social media road

In order to achieve the goals above selected, a key element will be to **invest in the community**, to build over a period of time a consolidated group that afterwards can be used to pass the message through in a swift and broad manner. This will certainly require effort and research to determine in advance who are the public that needs to be reached, how the message can be better delivered and finally what is the channel they are using.

In a more structural manner:

1) **Determine who is your target audience** (children, adults, enterprises, young professionals, elderly, etc. each group interacts in different social media channels depending on the country)

2) **Develop messages**
   
   o Each message released should have a purpose, normally in connection with the goals defined;
   
   o One message will not be enough to achieve results, but a consistent and constant stream of coherent messages is required;
   
   o When possible, use supporting material to complement and make your message more attractive (photos, videos, etc.) and quizzes or live questions & answers sessions to promote interaction. Be creative, exceed the expectations and use the element of surprise.

   The use of sense of humor and relaxed tone has been proven in certain cases as an excellent driver to better reach the public and transmit the message, especially when targeting young groups.

3) **Select the social media tool**, depending on the target audience and the kind of message you need to transmit
Avoid trying to drive a community to your preferred channel. Instead, use the channels your target audience is already using.

4) **Build up your community**
   - Social media is all about on-going dialogues, police need to interact with the target audience in law-enforcement related conversations;
   - Develop a corporate style/voice and presence and use existing connections to reach people. Communities expect police to address a number of themes; having a cybercrime specific channel may not necessarily be effective.

5. **Best practices**
   - **The community defines the channel and police need to go where the community is.** Social media channels change almost on daily basis. It is important to remain flexible and up to date on the latest developments, always scanning the communities that need to be reached out.
   - **Social media are characterised by a content driven engagement to help achieve asymmetrical communication with the public.** Police need to post real time, good, simple, accessible content in those channels where the targeted audience is. In occasions, it can be event driven as well, in those situations where the urgency or the importance of an incident or a fact will act as a driver it is crucial to get the facts right and only communicate them when they are clear and double checked.
   - **Police are to become social media professional users, building up a reputation of trust and credibility based on accurate content and constant presence.** The community expects law enforcement to act online just the same as they do offline, becoming and transmitting the feeling of center of (cyber) security.
   - **Police need to choose a suitable communication and wording tone depending on the targeted audience, adjusting it when changing from one community to another.** Timing can be relevant as well, since different communities connect at different times of the day.
   - **The security around the law enforcement social media account(s) is to be taken into consideration.** Besides strong credentials and limited access to only those who needed it, it is advised to check with the IT support team the requirements and conditions to ensure the Internet network access is properly protected.
   - **Coordination is key.** Due to the direct contact that social media generate with the public, the social media team needs to work closely with the police specialised units and investigators.
   - **Alignment among the various cybercrime fighting actors to avoid duplication and to strengthen the messages.** Law enforcement cannot combat cybercrime on its own. There are many partners from both public and private sectors also investing in cybercrime prevention and awareness efforts, including social media initiatives. Possibilities for cooperation are to be explored in order to send a single universal message, also including existing initiatives in the areas of online child sexual exploitation and payment fraud.
- **It is advisable to have a national “Community of Practice”, with a designated single point of contact (SPOC) for each of the social media channels at the various levels (national/regional/local).** Often, the social media platform providers (i.e. Facebook, Twitter, etc.) will have appointed SPOCs as well, to deal with the law enforcement community. These SPOCs will be different from the ones dealing with the investigative and operational side.

- **When it comes to targeting niche groups**, a way for police to show its presence is by placing advertisements to get messages across pages that are talking about the topic they want to tackle. This could be done with the goal to increase reporting of crime and to build confidence in the community.

- **Learning with the European Police College (CEPOL).** CEPOL offers a yearly course on Social Media implications for law enforcement. While the scope is much broader than the one covered by this Handbook, it can be considered as a good training experience to continue with social media education.

6. **Conclusions**

Social media policing is all about the service provided to the citizens. Law enforcement needs to focus on quality (am I being useful? am I covering their needs? am I bringing value?) instead of quantity (how many followers/posts do I have?).

While figures are important, reaching out successfully to the targeted community is yet even more important. Police will need to start by building up a serious profile and reputation; investing time and resources in mapping first the audiences and then the messages to transmit, and only then we will know what is the right social media channel to use per targeted group.

A successfully implemented social media strategy could bring exceptional results at the service of cybercrime communication, prevention and awareness; and not only that, could be a new source of information and intelligence to obtain operational results and increase the number of cybercrime cases reported.

7. **Useful links**

Would you like to enlarge your social media knowledge from a law enforcement perspective? Read more here:

- Facebook Politics & Government Case Study: Staffordshire Police
- www.policemediablog.com
- www.engageguide.net
- https://www.facebook.com/safety/groups/law/guidelines/
8. **ANNEX: About the law enforcement practitioners cooperating on this Handbook**

**Hellenic Police – Cyber Crime Division**

The mission of the Cyber Crime Division includes the prevention, investigation and suppression of crime and antisocial behavior, committed through the Internet or other electronic media. Cyber Crime Division is an independent central Division and reports directly to Chief of the Hellenic Police.

The Hellenic Cyber Crime Division consists of the following five departments: 1) Department of Logistics and Information Management, 2) Department of Innovative Actions and Strategy, 3) Department of Security of Electronic and Telephone Communications and Protection of Software and Intellectual Property Rights, 4) Department of Child Protection through Internet and Digital Investigation and 5) Department of Special Affairs and Prosecution of Internet Financial Crimes

Social media channels used:

- Facebook: [https://www.facebook.com/cyberkid.gov.gr](https://www.facebook.com/cyberkid.gov.gr)
- Facebook: [https://www.facebook.com/CyberAlertGR](https://www.facebook.com/CyberAlertGR)
- Twitter: [@CyberAlertGR](https://twitter.com/CyberAlertGR)
- YouTube: [https://www.youtube.com/channel/UCMtEyQaJq8RIZONuo7Q38g](https://www.youtube.com/channel/UCMtEyQaJq8RIZONuo7Q38g)

Social media role:

The presence of the Cyber Crime Division on social media, when it comes to raising awareness and providing citizens with information on internet safety, risks and threats while being online, could be divided into two major pillars:

The first one is the “CyberKid” campaign, launched in 2011 with the creation of the site [www.cyberkid.gr](http://www.cyberkid.gr). This campaign has been developed to inform basic Internet users, in particular parents, teachers and children, about Internet safety. The Facebook page “CyberKid” informs citizens on daily basis about new threats and developments.

The second is the “CyberAlert-Feelsafe” campaign, which aims at more advanced Internet users and businesses. In this context, the Hellenic Cyber Crime Division and the National Confederation of Hellenic Commerce signed a Memorandum of Cooperation to promote and coordinate actions in favor of fair organized trade and consumers. In the framework of this campaign, the Twitter account “@CyberAlertGR” and the Facebook page “CYBER ALERT” not only inform Internet users on new threats and trends but it give them the possibility to report emergency cases. Additionally, useful videos produced by the Division are uploaded on the YouTube channel “CYBER ALERT”.

Social media team:

The Cyber Crime Division of the Hellenic Police pays particular attention to the area of cybercrime prevention and awareness. In 2014, the Innovative Actions
and Strategy department was developed, which is in charge of the planning and implementation of awareness activities and communication with both public and private sectors. This department is responsible for the social media profiles of the Division. The department consists of five special duty officers (all with relevant Computer Science background) and supportive general duties officers. The staff of the department works six days a week and seven hours a day on the described actions. Additionally, a specialized laboratory works on the development of innovative applications (apps).

**Polizia di Stato – National Cybercrime Police**

The Italian National Police is the national civilian police force of Italy. Under the authority of the Italian Ministry of Interior, the Postal and Communications Police represents the competent authority for the prevention of and response to cybercrime, since it was established following the reform of the Public Security Administration, and it is also the body in charge of safeguarding the privacy and freedom of any form of correspondence and communication among citizens.

Social media channels used:

- Facebook: [https://www.facebook.com/poliziadistato.it](https://www.facebook.com/poliziadistato.it)
- Twitter: @poliziadistato
- YouTube: [https://www.youtube.com/user/poliziadistato](https://www.youtube.com/user/poliziadistato)

Social media role:

- Information sharing;
- Education of citizens, especially the younger people on phenomena such as cyber-bullying and on-line grooming;
- Facilitate the contact with victims of criminal activities;
- Information gathering for investigative purposes;
- Co-operation with foreign law enforcement agencies.

Social media team:

The social media team is part of the Central Corporate Communication Unit. All its members are police officers specialized in communication. The Central Corporate Communication Unit shares with other specialized units within the Italian National Police such as Cybercrime Units, Drugs Units, and Illegal Immigration Units knowledge on new criminal trends, *modus operandi* and operational activities.

**Spanish National Police**

The Spanish National Police is the national civilian police force of Spain. Under the authority of Spain’s Ministry of Interior, it is mainly responsible for policing urban areas. The Spanish National Police mostly handle criminal, judicial, terrorism, public safety, forensic and scientific and immigration matters. It is deployed to the whole territory with central and peripheral units. Nowadays the main priorities for the Spanish National Police are preventing and combating cybercrime, serious
and organised crime, terrorism, illegal immigration and trafficking of human beings and drug trafficking.

Social media channels used:

- Facebook: https://www.facebook.com/PoliciaNacional
- Facebook: www.facebook.com/BrigadaInvestigacionTecnologica
- Twitter: @policia
- YouTube: https://www.youtube.com/user/Policia
- Instagram: https://instagram.com/policianacional/

RSS Channels (users can subscribe to these feeds to receive updates when their content changes):

- http://www.policia.es/rss/actualidad.xml (Police news)
- http://www.policia.es/rss/alertas.xml (Cyber alerts)

Social media role:

- Awareness raising on existing and future threats and criminal trends;
- Prevention and dissuasion for potential criminals;
- Education;
- Public Protection for potential victims;
- Protection and reaction for victims of criminal activities;
- Information sharing;
- Information gathering for investigative purposes.

Social media team:

The Social Media team is part of the Press Office and Public Relations central Unit. All its members are police officers specialised in communications. The Press Office and Public Relations Unit works in cooperation with specialised police units such as the Cybercrime Units, Drugs Units, Illegal immigration Units, etc. in order to have an updated knowledge, legal advice and a close view on new modus operandi, criminal procedures, investigation possibilities, existing and future threats and criminal trends, etc.

@policia, the department’s Twitter account, has become the most popular in the world maintained by a law enforcement agency, with nearly two million followers in a country of 47 million people.

**UK National Crime Agency**

The National Crime Agency leads UK law enforcement’s fight against serious and organised crime. It has built multi-agency partnerships across police, law enforcement, the public sector, private industry and internationally to lead, support and coordinate the UK’s response to a wide range of threats.
Social media channels used:

- Facebook: [https://www.facebook.com/NCA](https://www.facebook.com/NCA)
- Twitter: @NCA_UK
- LinkedIn: [https://linkedin.com/company/national-crime-agency](https://linkedin.com/company/national-crime-agency)
- YouTube: [https://www.youtube.com/user/NationalCrimeAgency](https://www.youtube.com/user/NationalCrimeAgency)
- Flickr: [https://www.flickr.com/photos/ncauk/albums](https://www.flickr.com/photos/ncauk/albums)
- Tumblr: [http://national-crime-agency.tumblr.com](http://national-crime-agency.tumblr.com)

Social media role:

Social media is recognised as one of NCA’s most effective tools for reaching and engaging communities online. Social media is used in many different ways, from public safety messaging to Most Wanted appeals, undermining criminal operations and demonstrating operational successes. Where possible, the agency tries to create a dialogue with users (particularly authoritative figures) in order to build positive relationships and influence behavior.

Social media team:

Social media is managed by the Digital team within External Communications. They work closely with the wider Communications team and the agency at large to ensure they serve operational priorities. Individual officers are encouraged to use social media in both a personal and professional capacity in order to broaden the agency’s social footprint and to engage with communities.

**UK Staffordshire Police**

It provides a policing service to the people of Staffordshire and Stoke-on-Trent. The force area includes one of the largest shire counties in England, covering more than 2,600 square kilometers or 1,000 square miles. It has a population of more than 1,000,000 and a rich diversity of communities, all with their own specific policing needs.

Social media channels used:

- Facebook: [https://www.facebook.com/staffordshirepolice](https://www.facebook.com/staffordshirepolice)
- Twitter: @StaffsPolice
- YouTube: [https://www.youtube.com/user/staffordshirepolice](https://www.youtube.com/user/staffordshirepolice)
- Flickr: [https://www.flickr.com/photos/staffordshirepolice/](https://www.flickr.com/photos/staffordshirepolice/)

Social media role:

Social media is a central part of the forces daily activity, and it is fully integrated into the force communications and engagement strategy and tactics. The Head of Press Office/Media coordinates and develops the use of the platforms. There is a strong use of analytical and insight data to make evidence based decisions on effectiveness.
Social media team:

It is led by the media and communications team but with access delegated to local officers, control room and specialist teams.

With a strong geographic focus, Staffordshire Police are widely acknowledged as being a leading force in the use and application of social media, as well as the first source of information likely to be consulted and trusted in the area.