Corporate Policy | Service Instruction

SI1017

PSNI Social Media

SI Identification Number	SI0117
Policy Ownership	Strategic Communications and Engagement
Initial Publication	21/02/2017
Review Cycle	5 Years
Reviewed	06/07/2023
Last Amended	N/A
Governing Service Policy	Strategic Communications and Engagement
Cancellation of	N/A
Classification	**OFFICIAL [PUBLIC]**

The Police Service of Northern Ireland's strategic aim in using social media is to engage professionally with the public, partners, stakeholders and media.

Table of Contents

1. Introduction....4
2. Police Service of Northern Ireland Social Media Channels....4
3. Training....5
4. Access and Application....5
5. Governance & Strategic Communication and Engagement Department (SCED)....7
6. When Using Social Media....10
7. Security When Using Social Media....11
8. Media....11
9. Crimes, Complaints and Concerns....12
10. Images....12
11. Private Messages (PMs)....13
12. Posts/Comments to the Pages....14
13. Inappropriate Posts/Comments....14
14. Hashtags....15
15. Competitions....15
16. Missing Persons (MP)....15
17. Mistakes/Errors....16

Table of Appendices

Appendix A Ten Golden Rules 18

Appendix B Social Media Appropriate Guidance 24

Appendix C Contact Details.....26

1. Introduction

This Service Instruction promotes the responsible use of Police Service of Northern Ireland social media by trained users within the Service, while also empowering them to take advantage of the broad engagement opportunities afforded by social media whilst managing associated personal and organisational risks. It helps ensure the use of social media by Police Officers and Police Staff is effective, safe, and appropriate, while enhancing the reputation and professional integrity of the Police Service.

Social media enables Police Officers and Staff to be accessible and visible to their communities and can be used as an effective means to positively impact on the achievement of operational or corporate objectives.

Police Service of Northern Ireland social media should be used to:

- Share information about policing;
- Prevent, detect and deter crime;
- Provide reassurance around crime and the fear of crime;
- Promote the Service;
- Develop and strengthen community, stakeholder and business engagement;
- Improve and build confidence in policing;
- Develop trust in the Service;
- Promote the Service's brand identity and values;
- Provide timely, relevant and accessible information; and
- Support Operational Policing.

Police Service of Northern Ireland social media should be a trusted source of information for the public.

2. Police Service of Northern Ireland Social Media Channels

The Service has a number of Corporate and District social media channels including:

- Facebook;
- Twitter;
- Instagram;

- LinkedIn;
- YouTube; and also
- Access to Nextdoor.

The Strategic Communication and Engagement Department (SCED) will create content and post on these when relevant and appropriate.

SCED will have access to all police social media accounts (Facebook, Twitter, LinkedIn and Instagram) for audit, management and governance purposes.

3. Training

Training is mandatory for all PSNI Officers and Staff who use official PSNI social media channels. To access Police Service of Northern Ireland social media, Officers and Staff must complete the social media training, delivered by SCED's Digital Hub who will maintain records of Social Media and 'Nextdoor' training.

Any application for external training provision should be discussed and agreed with the Digital Hub prior to any procurement process.

4. Access and Application

Social Media

Authorised social media users in Districts / Departments can only access Police Service of Northern Ireland social media (Facebook, Twitter and Instagram) through a social media management platform. To gain access they must make a request to their District / Department Single Point of Contact (SPOC), who will keep a record of it.

Nextdoor

Authorised 'Nextdoor' users in Districts / Departments can only access Nextdoor when an official police account has been created for them. To gain access they must be a Neighbourhood Policing Officer and must make a request to their Line Manager who will keep a record of it.

The Digital Hub

The Digital Hub will liaise with the SPOC and Neighbourhood Teams annually to identify user provision gaps and new social media / 'Nextdoor' users. They will arrange training and the creation of a 'social media management platform' / 'Nextdoor' account for all new users.

The social media management platform are not accessible through a common terminal. They can be accessed through Samsung devices and Nextdoor can be accessed through a standalone computer.

Devices

All devices used for social media must be enrolled in a mobile device management (MDM) system by contacting Information and Communications Services (ICS) and requesting a device set up for social media use. If a device becomes locked it must be reported to ICS as a rebuild for social media access.

Devices are purchased and owned by Districts / Departments and it is their responsibility to:

- Monitor placement and use,
- Ensure that devices are fit for purpose and updated when appropriate.

New Social Media / Digital Channels

Any District, Department or individual who requests a new social media channel will be required to utilise existing Police Service of Northern Ireland social media channels for a minimum of six months to demonstrate sustainability and an appropriate level of engagement before an application for a new channel will be considered.

Application for new social media / digital channels (e.g. a new Facebook page or Twitter feed) **must** be made in writing to the Head of Digital Engagement and Creative (SCED).

The application will be presented to the Senior Executive Team with a recommendation from Head of Digital Engagement and Creative (SCED). The Senior Executive Team will make the final decision on approval or rejection.

Any application should clearly state;

1. The business purpose;
2. Aims and objectives;
3. Risks;
4. Mitigating factors;
5. Details of current social media use; and
6. How the new channel will contribute to the strategic aim of social media use by the Service.

New social media channels will be created by the Digital Hub and will follow Police Service of Northern Ireland branding and style guides.

If a social media channel, social media management platform account or Nextdoor account is no longer required it is the responsibility of the account holder to inform the Digital Hub via email.

Associations or Affiliated Groups

Social media channels for Associations or affiliated groups do not fall under the remit of SCED, however the Digital Hub must be made aware when a channel of this nature is created. The creation, management and ownership of such channels sits with the Association or group.

All such channels must include the following line in their bio: '*views expressed and content shared do not reflect the corporate position of the Police Service of Northern Ireland'.*

5. Governance & Strategic Communication and Engagement Department (SCED)

Police Service of Northern Ireland social media is governed by Strategic Communication and Engagement Department (SCED), in partnership with the Senior Executive Team (SET).

Governance
SCED will:
• Shape and direct the development of Police Service of Northern Ireland social media and address any challenges or issues that arise;

- Provide direction, advice, support and guidance to the command teams and social media users;
- Delete inappropriate posts without notification or consultation.

District / Departments will:

- Disseminate information and direction from SCED
- Hold regular social media user meetings regarding direction and guidance from SCED;
- Feed information back to SCED through the Digital Hub;
- Appoint a SPOC

SPOC who will:

- Monitor social media performance for their specific area.
- Ensure that the social media Service instruction and Social Media Standards are adhered to;
- Monitor and respond to Private messages;
- Ensure Social Media is used appropriately by users in their area of responsibility.

The Digital Hub will:

- Be responsible for the management and oversight of all official Police Service of Northern Ireland social media channels;
- Attend all social media user meetings;

- **Suspend, revoke or delete user access and/or an account** without notice or consultation if it is believed to be representing an organisational risk or bringing the service into disrepute;
- Delete any unauthorised accounts; and provide
- Support and guidance to all social media users as required in relation to content, devices and engagement.
- District / Department command teams with regular information/updates/statistics on social media performance, developments and changes;
- Direction and guidance around communications on social media channels to social media users and District / Department command teams;
- Information to;
  - The Head of Digital Engagement and Creative,
  - Director of Strategic Communication and Engagement Department and
  - ACC District Policing Command to inform the Senior Executive Team.
- Suspend, revoke or delete access and/or account without notice or consultation if a user and/or account is believed to be representing an organisational risk or bringing the service into disrepute.
- No unauthorised accounts should be set up and if so the Digital Hub will seek to delete these.

6. When Using Social Media

It is important to consider whether social media is the appropriate form of communication and if so the tone of the content must be considered.

Language and tone on all social media posts must be professional and factual and every post must be considered as a formal statement from the Service.

All Police Service of Northern Ireland social media users are governed by:

- The Social Media Standards;
- Ten Golden Rules (Appendix A);
- The Code of Ethics; and
- NICS Standards of Conduct.

Any breach of these rules or standards will be reported to the relevant authority for consideration and/or investigation.

Content posted on social media must align with the aims outlined in the introduction and must be presented in a tone, style and manner which adheres to Police Service branding and values. Content must be appropriate and must not be used to disclose or process sensitive Service information.

Content **should not** be posted if it:

- Contains protectively marked or sensitive information;
- May be libellous;
- Contains information that may be subject to copyright or intellectual property rights;
- Contains operational sensitive information;
- Contains commercially sensitive information;
- Breaches confidentiality;
- Damages the reputation of the Service or acts against the Services' best interests;
- Could identify (directly or indirectly) living persons (except in the case of missing persons);
- Is; defamatory, racist, sexist, obscene, or otherwise likely to cause offence, or;
- Is religiously or politically biased.

The above is not in place to restrict free speech, but to illustrate the standard of engagement and communication expected of Police Service of Northern Ireland social media users.

SCED monitor Police Service accounts and conduct wider environmental scanning. This assists in identifying any emerging community issues enabling us to respond appropriately to any rumours, concerns or complaints from the public.

Pages that imitate the Police Service and use copyright material **must** be reported to the Digital Hub via email. A report will then be forwarded to the social media provider.

If you have any queries contact the Digital Hub.

7. Security When Using Social Media

Police social media account passwords are held securely by SCED.

Passwords to social media management platform accounts are retained by the individual user and should not be shared with colleagues. Passwords **must** be changed regularly (at least annually) and **must** contain at least one uppercase letter, symbol and number.

All social media users should ensure that they log out of their social media management platform account when using a shared device to ensure their account is not unwittingly used by another.

Employees should be conscious of the fact that any content displayed on social media is considered to be in the public domain.

Personal devices **must not** be used to access Police Service of Northern Ireland social media, either directly or through the social media management platform (with the exception of Facebook admin account holders).

8. Media

Any activity and/or information in the public domain is a potential and legitimate source of media interest.

SCED should be contacted if media outlets request further information about a post or

request media contact such as interviews, visits or ride-alongs.

Social media users should also contact the News and Media Room on Ext 70750 if they believe it is likely or if it becomes apparent that a post will generate media interest.

9. Crimes, Complaints and Concerns

Social media should not be used to report; crimes, incidents or lodge a complaint. Complaints must be forwarded to the Police Ombudsman for Northern Ireland or the relevant Head of Department. Automated responses for private and direct messages are in place on each social media feed to clarify the reporting procedure through the 101, 999 or non-emergency online reporting form.

Concerns for safety, missing persons, vulnerable persons or any Article 2 European Convention on Human Rights (ECHR) issue must be dealt with as a matter of urgency.

A screenshot of the message/post that gives rise to concern must be forwarded to Contact Management Centre (CMC) immediately and contact made to commence a Control Works.

10. Images

When creating a social media post best practice (if possible) is to include images, videos, and animations to increase the likelihood of a user seeing the post on their timeline.

In line with General Data Protection Regulation (GDPR) images of people taken in the course of duty must only be uploaded with the individual's permission or with the permission of a person who has parental or guardian responsibility. This permission is also required from colleagues prior to you posting images containing them. A signature clearly stating their agreement to that effect must be recorded in a Police notebook or GDPR permission card;

Examples of how to record this permission are as follows:

"I have viewed the image and I agree to it being used in Police Service of Northern Ireland social media."

"I have viewed the image and I …….. have parental/guardian responsibility for and or the ……..School/Youth Group and agree to it being used in Police Service of Northern Ireland social media."

Care must be taken not to identify personal details in photographs. This includes house numbers, and any identifiable logos, business names or registrations on vehicles, unless this is relevant to an appeal and with the person's consent.

Images should not be taken from the internet to prevent any copyright breaches. All images, graphics and footage used on Police Service of Northern Ireland social media must follow the corporate brand guidelines.

Photographs taken within police establishments must adhere to Security Branch policy. Images or information posted on any social media site must comply with the National Police Council (NPCC) Guidance on the release of images of suspects and defendants and on the release of evidential material, legislation such as:

- Data Protection Act 2018:
- General Data Protection Regulation (GDPR):
- Police NI Act 2000:
- The Contempt of Court Act: 1981:
- Copyright and Patents Act 1988:
- Children (NI) Order 1995:
- Sexual Offences (NI) Order 2008:
- Any other relevant law.

Guidance on the release of images of suspects and defendants through media and digital platform document can be obtained by contacting SCED's news and media room.

11. Private Messages (PMs)

Switching on the private message function on local social channels is a decision for the relevant District/Department whose

social media users will be responsible for monitoring and responding to messages.

All PMs must be responded to within a reasonable timeframe. Operational commitments will dictate this timeframe but good practice is to respond on the same day.

Private messages should be monitored by all social media users in the relevant Department or District when they are on duty.

It is the responsibility of the social media user who opens a PM to act accordingly and ensure it is replied to.

Should further consultation be required, then a response to the person should be sent to inform them, while reassuring them they will be updated as soon as possible.

If any Freedom of Information (FOI) requests are received through PMs these must be forwarded to the Freedom of Information Branch immediately. Ensure that contact details are also forwarded in the mail.

12. Posts/Comments to the Pages

Posts and comments made to the page **must** be monitored and where appropriate answered.

13. Inappropriate Posts/Comments

Inappropriate posts/comments to the page must be screenshot and the posts/comments deleted.

If you do not have the ability to screenshot on your work device you must contact the Digital Hub or Press Office for assistance.

The Digital Hub must be made aware of any deleted post and screenshots of the deleted post and comments should be emailed to the Digital Hub so that they can be recorded and filed appropriately. Inappropriate posts/comments can be defined, yet not limited to the guidance found in Appendix B.

Consideration may be given to:

- Banning the user;

- Reporting the post/comment to the social media provider; and/or
- Beginning an investigation for potential criminal offences.

This should be done through discussion with the Digital Hub.

14. Hashtags

The Police Service of Northern Ireland has three hashtags, which must be written in the style below paying attention to the use of capital letters:

i. #PSNI

ii. #KeepingPeopleSafe

iii. #WeCareWeListenWeAct

The first letter of each word in a hashtag must be upper case to facilitate accessibility.

Social media users must not create or use their own hashtags

Should an event, ongoing social media plan or corporate campaign require the use of a bespoke hashtag, an application **must** be made to the Digital Hub to authorise the use. The application must contain;

i. The hashtag desired;

ii. Event details, and;

iii. Evidence of research conducted to ensure the hashtag does not have any inappropriate associations on social media.

Applications **must** be made at least 3 days in advance of the proposed use and sent via email to the Digital Hub.

15. Competitions

Competitions **MUST** be open and transparent and approved by SCED.

16. Missing Persons (MP)

In a missing person enquiry the use of social media may be considered, due to the valuable resource of an extensive follower base.

It will be the responsibility of the Investigating Officer (IO) to ensure that suitable provision is made for monitoring of

comments made by the public and PMs in relation to a missing person appeal. When a missing person is located the original post containing their information and photograph must be deleted, but only after their next of kin has been made aware that they have been located. Deletion should be recorded on the missing person Occurrence Enquiry Log (OEL).

Screenshots of the deleted post and any attached comments must be made prior to the deletion and forwarded to the Digital Hub so they can be recorded and archived appropriately.

If you do not have the ability to screenshot on your work device you must contact other social media users in your district/department in the first instance for assistance. If no other social media user is available you must contact the Digital Hub or the Press Office for assistance.

An update post must be posted onto the same social media page.

Where a missing person is **located safe and well the message should read**:

- Thank you for your help with our missing person appeal from earlier. They have now been located.'

Or – Where a missing person has been **located deceased the message should read**:

- Thank you for your help with our missing person appeal from earlier. This appeal is now cancelled.'

17. Mistakes/Errors

If a social media user makes a mistake/error, steps **must** be taken to rectify it as soon as practical. For example if incorrect information is posted, a screenshot of the post **must** be taken, the mistake/error acknowledged, apology made and finally the correct information posted.

Screenshots of the post and any attached comments must be made prior to deletion and forwarded to the Digital Hub so they

can be recorded and archived appropriately.

The line manager **must** be made aware of the incident. If the mistake/error is likely to generate media attention, then SCED **must** be contacted.

Where a mistake/error is a matter of misconduct, it should be dealt with through the standard disciplinary procedure.

If a member of the public makes a complaint about a mistake/error attempt to resolve it locally but if this is not possible, the incident **must** be referred to the Police Ombudsman Northern Ireland.

Appendix A Ten Golden Rules

10 Golden Rules

1. The same standards of conduct apply online as offline;

When you use social media as a representative of Police Service of Northern Ireland, you should always be professional, respectful, fair and courteous and work within the parameters of the Code of Ethics and the NICS Code of Conduct.

The Code of Ethics

The Code of Ethics underpins the fundamental policing purpose of keeping people safe; this should be reflected in every interaction on social media. The ethical standards outlined in the code should be applied to our use of social media to demonstrate the highest standards of integrity and professionalism.

All social media users should adhere to the following sections of the Code of Ethics:

1.10: Whether on or off duty, Police Officers shall not behave in a way that is likely to bring discredit upon the Police Service; and

6.1: Police Officers shall act with fairness, self-control, tolerance and impartiality when carrying out their duties. They shall use appropriate language and behaviour in their dealings with members of the public, groups from within the public and their colleagues. They shall give equal respect to all individuals and their traditions, beliefs and lifestyles provided that such are compatible with the rule of law.

Civil Service Standards of Conduct

The following core values of the Civil Service Standards of Conduct should also be reflected in our interactions on social media:

- Always act in a way that is professional and that deserves and retains the confidence of all those with whom you have dealings; and
- Deal with the public and their affairs fairly, efficiently, promptly, effectively and sensitively, to the best of your ability.

2. Do not ignore your followers:

Social media is a vital engagement tool for the Service and engagement is a two way street – we must talk, listen and respond.

If you post content and members of the public respond, you must monitor responses and respond accordingly. Even if no response is required, a simple like on the comment can let the public know that you have heard what they are saying.

When engaging with the public through comments or private/direct messages you must always be polite and respectful. You should never be patronising, arrogant or dismissive.

If someone asks you a direct question, you should answer it to the best of your ability. If you don't have the information at the time, answer and say you're going to check and come back to them with an answer.

If a debate starts it is fine to monitor how the conversation is going. Often when there is criticism of Police, other followers will come into the conversation and defend Police actions, negating the need for us to enter the conversation. In other instances, if criticism of our actions is overwhelming we have a responsibility to engage. This can seem daunting but you can seek advice from the Digital Hub or discuss with a Senior Officer before responding.

Private messages must be monitored on a daily basis and answered. A private message is akin to a member of the public phoning or calling to an enquiry office so our response and the time it takes to respond has a direct impact on their confidence and trust in policing.

3. Do not criticise a Judges' sentencing or enter into a discussion about legal proceedings or outcomes.

It is not appropriate for Police to comment on the practices, decisions or operational choices of criminal justice and other partners or stakeholders.

Information contained in posts/comments/messages should be based solely on police activity.

4. Do not talk politics

Police Service of Northern Ireland social media should not be used to share your own personal views on politics or any other matter.

You are posting on behalf of the Chief Constable so all information shared must reflect Service's corporate position on the specific issue.

5. Do not post personal or protectively marked information.

All information shared on Police Service of Northern Ireland social media must align with data protection regulations.

Photographs must align with GDPR regulations and permission must be sought from individuals (**whether members of the Public or Police Officers/Staff**) before their image is posted onto PSNI social media. This does not apply in the case of wanted individuals or where it has been agreed to share images of convicted criminals. The release of images permission process must be followed in these instances. It also does not apply to missing people. Best practice for missing people is to request permission from a family member for

an image to be used. If a request is refused, operational need and the risk level will dictate the requirement to release a photo.

Care should be taken with all photographs taken within the police estate. You must ensure that no protectively marked information appearing on computer screens, posters or paperwork is viewable in the photo.

If you are taking a picture in the car park of a police estate you must ensure that all vehicle registration plates or easily recognisable vehicles are blurred out.

6. Always be professional, respectful and dignified (no sarcasm).

Be polite to our followers. Each and every member of the public deserves to be treated with respect. While humour is acceptable and usually well received on our social media you must always be cautious that it does not create the perception of derogatory or disrespectful commentary.

If a follower is being rude or offensive, this should be met with dignity and respect.

Profanity filters on our social media feeds mean that comments containing bad language will not be displayed on our feeds.

7. Do not use personal devices to post from Police Service of Northern Ireland accounts.

The social media management platform should only be accessed through a Police Service of Northern Ireland issued device – usually a Samsung phone, idevice or **stand-alone** computer.

The social media management platform, for the purposes of accessing police social media, should not be accessed from a personal phone or device.

8. Do not compromise operational activities.

Details of police activity, particularly joint operations between different Police Service of Northern Ireland departments, should only be shared with the permission of all relevant departments.

In most cases, details of planned operations should only be shared;

- After the fact; or
- While an operation is ongoing **if** there is a specific reason to do so ahead of time.

If you are posting information about a serious crime, you must agree wording and content with the Senior Investigating Officer.

You should not comment on or make reference to police operations in other Districts/Departments unless specifically requested to do so.

Best practice is to contact the department with specific ownership of an area of business before posting about it eg if you are posting about domestic abuse, you should contact Public Protection Branch.

9. All posts must have a policing purpose. Do not promote personal activities, interests or preferences.

Every social media post must have a clear and evident policing purpose. Before you publish content you should be clear on what the aim of the post is, who your target audience is and what you hope to achieve.

Our core aims on social media are: to improve confidence in policing, to develop trust in the Service, to encourage dialogue and interaction between us and our communities and to establish our social media channels as trusted sources of information.

Content should always be in the interest of the Service.

Posts should not be **self-serving** and should never be used for **self-promotion**.

Social media users should not share**;** personal opinions**,** personal information or promote or name businesses.

10. Use common sense and plain English.

Social Media users should:

- **Avoid 'police speak',** (While you may be used to acronyms, the public may not understand what they mean**);**
- **Check all grammar**, spelling and punctuation before posting.
- **Not use slang**.
- **Ensure content** on your social media feed **is** relevant to the local area.
- **Not use sarcasm**, offensive language or disparaging comments.

Appendix B Social Media Appropriate Guidance

Social Media Appropriate use Guidance	
i.	No offensive posts;
ii.	No Political posts;
iii.	No religious posts;
iv.	No swearing;
v.	No comments that would hinder or jeopardise live investigations;
vi.	No advertising;
vii.	No naming of any specific person or business;
viii.	No complaints against Police Officers;
ix.	No threats;
x.	No obviously inflammatory comments;
xi.	No inciting criminal activity;
xii.	No discriminatory posts; and
xiii.	Not to be used to report crime.

Posts which do not comply with Facebook terms or are deemed to be offensive, discriminatory, and accusatory or incite criminal activity will be deleted. The Police Service of Northern Ireland is not responsible for content posted up by members of the public.

Appendix C Contact Details

Service Instruction Author

Digital Hub

Branch Email

CorporateComms-PressOffice@psni.police.uk