Corporate Policy

SERVICE INSTRUCTION

SI Identification Number	SI1017
Policy Ownership	Corporate Communications
Issue Date	21/02/2017
Review Date	5 years from issue date
Governing Service Policy	Corporate Communications
Classification	**OFFICIAL [PUBLIC]**

SI1017

Social Media

The Police Service of Northern Ireland supports its Police Officers and Police Staff in the responsible use of social media both for business and personal use. This Service Instruction helps ensure the use of social media by Police Officers and Police Staff is effective, safe, and appropriate, while enhancing the reputation and the professional integrity of the Police Service. The use of social media is for engagement purposes, environmental scanning, enhancing other operational activity and to support the Chief Constable's vision.

Keeping People Safe

Table of Contents

1. Introduction

With the increasing use of social media this Service Instruction promotes the responsible use of social media by all employees of the PSNI, while also empowering trained users to take advantage of the broad engagement opportunities afforded by social media whilst managing associated personal and organisational risks.

Social media can be used as an effective means to significantly impact on the achievement of operational or corporate objectives. This means of communication can also improve relationships with staff, stakeholders, customers and the public.

2. Training

Training is available for all employees who use social media as part of their work. To access PSNI social media accounts employees must have completed Social Media Awareness and Hootesuite training. District training teams will ensure that eServices qualifications are updated on completed training.

Title and Ref number of Training Courses

Social Media Awareness 50238667DT022

Hootesuite Training 50238668DT023

3. Access and Application to PSNI Social Media

To access social media as part of your daily duties, an application by a supervising officer of at least Inspector/Staff Officer Grade in writing using form DH1 must be completed and submitted via email to zSocialMedia. These forms are available on Policenet by visiting the Digital Hub page on the Corporate Communications section.

Application for new social media/digital accounts **must** be made in writing to the Head of Corporate Communications Department (CCD) who will make a decision on whether to grant the application. Any application should clearly state;

i. The business purpose;

ii. Aims and objectives;

iii. Risks;

iv. Mitigating factors, and;

v. How the new account will contribute to the Chief Constable's (CC) vision.

New accounts will be set up by Corporate Communication and will follow PSNI style guide.

If a social media account is no longer required it is the responsibility of the account holder to inform zDigitalHub via email.

4. Corporate Communication Department (CCD)

CCD will delete inappropriate posts without notification or consultation.

CCD will suspend revoke or delete access without notice or consultation if a user is believed to be representing an organisational risk/ or bringing the service into disrepute.

CCD will delete a social media account if it has been compromised and presents organisational risk or reputational damage to the Police Service.

No unauthorised accounts should be set up. CCD will seek to delete these and report the matter to Discipline Branch.

5. Personal Safety

Identifying that you work for the PSNI (or have a connection to it) on a personal social media account or page may carry a degree of tangible risk.

For example, you could become a target for attack, be targeted for information, blackmailed or render yourself family and friends vulnerable to personal threats.

Employees are advised to use their discretion in identifying their employment online.

6. When Using Social Media

It is important to consider whether social media is the appropriate form of communication, if so the tone of the content must be considered. An informal, friendly, light hearted tone is acceptable provided standards of behaviour are upheld. Ten Golden Rules to consider when using social media are provided in Appendix A.

Content posted on social media must be appropriate and must not be used to disclose or process sensitive Service information. The following points identify content that **should not** be posted;

i. Contains protectively marked or sensitive information;

ii. Be libellous;

iii. Information that may be subject to copyright or intellectual property rights;

iv. Operational sensitive information;

v. Commercially sensitive information;

vi. Breach confidentiality;

vii. Damage the reputation of the Service or act against the Services' best interests;

viii. Information that could identify (directly or indirectly) living persons (except in the case of missing persons);

ix. Be defamatory, racist, sexist, obscene, or otherwise likely to cause offence, or;

x. Be religiously or politically biased.

The above is not in place to restrict free speech, but to illustrate as representatives of the Service, officers and staff need to uphold an appropriate standard on social media.

CCD shall monitor Police Service accounts using 'Tweetdeck' and 'Hootesuite' and may pick up wider references to PSNI. This assists in identifying any emerging community issues enabling us to respond positively to any rumours, concerns or complaints from the public.

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

If in doubt contact CCD.

7. Security When Using Social Media

Personal devices **must not** be used to update PSNI social media.

PSNI social media account passwords are held securely by Corporate Communication Department (CCD) and shall not be shared under any circumstances.

Passwords to Hootesuite accounts will not be shared with colleagues. Passwords **must** be changed regularly (at least annually) and **must** contain at least one uppercase letter, symbol and number.

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

8. Media

'@ message' Tweets and Facebook updates are all public unless it is a private and publicly hidden person-to-person exchange, such as via 'Direct Message'.

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

Corporate Communications should be contacted if media outlets request further information about a post.

Social media users should also contact the CCD Press Desk on x21150 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 or calls. If a person attempts to report crime a response must be made to clarify the reporting procedure through the 101, 999 or non-emergency online reporting form. If a crime has been reported, steps must be taken to address Article 2 ECHR immediate risk/threat to life.

Social media should not be used to lodge a complaint. Complainants must be forwarded to the Police Ombudsman for Northern Ireland or the Head of Department.

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 rises to concern must be forwarded to Contact Management Centre (CMC) immediately and contact made to commence a Command and Control(C&C) serial.

10. Images

Best practice (if possible) is to include an image with a post; this will increase the likelihood of a user seeing the post on their timeline.

Images of persons taken in the course of duty must only be uploaded with the person's permission or with the permission of a person who has parental or guardian responsibility. Permission must be sought from colleagues prior to posting images containing them. A signature to that effect must be recorded in a police notebook clearly stating their agreement.

Examples of how to record this permission are as follows;

"I have viewed the image and I agree to it being used in PSNI 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 PSNI social media."

Care must be taken not to identify personal details in photographs, this includes house numbers and vehicle registrations, unless this is relevant to the appeal and with the person's consent.

Images taken from the internet may be owned or subject to copyright. These images can only be used with the owner's permission.

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 the Contempt of Court Act, Copyright and Patents Act, Children and Young People's Act, Sexual Offences Act and any other relevant law.

11. Following/Liking Accounts

It is recommended to follow partner agencies, local community organisations and news outlets. Care and consideration should be taken when following individuals, e.g. if you follow a local councillor, it is recommended you follow all local councillors. This shall strengthen relationships and avoid confusion.

Encourage people, businesses, and organisations to follow your feed. Maximise opportunities to increase your follower base at appropriate times.

12. Private Messages (PMs)

PMs are confidential unless explicitly stated by the user and the accounts are for engagement only.

All PMs must be responded to within a reasonable timeframe. Operational commitments will dictate this timeframe but a guide should be for a response to be sent the same day.

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 ZFOI immediately. Ensure that contact details are also forwarded in the mail.

13. Posts/Comments to the Pages

'Post to Page' function **must** remain active on all active accounts unless directed otherwise by CCD.

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

14. Inappropriate Posts/Comments

Inappropriate posts/comments to the page must be screenshot and the posts/comments deleted. Inappropriate posts/comments can be defined, yet not limited to the guidance found in Appendix B.

Consideration may be given to banning the user and in addition report the post/comment to social media provider and/or begin an investigation for potential criminal offences.

15. Hashtags

The PSNI have two hashtags, which must be written in the style below paying attention to the use of capital letters:

i. #PSNI

ii. #KeepingPeopleSafe

Should an event require the use of a bespoke hashtag, an application **must** be made to CCD 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 zDigitalHub.

16. Competitions

Must be open and transparent and approved by CCD.

17. 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. Deletion must be recorded on the missing person log and C&C updated accordingly.

An update post must be posted onto the same social media page eg ‘Thank you for your help with our missing person appeal. This person (or you can insert name of missing person) has been located.’

18. 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.

The line manager **must** be made aware of the incident. If the mistake/error is likely to generate media attention, then CCD **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 make a complaint about a mistake/error attempt to resolve locally. If this is not possible, the incident **must** be referred to the Police Ombudsman Northern Ireland.

Appendix A Ten Golden Rules

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

2. Do not ignore your followers;

3. Do not criticise a judges sentencing or enter into a discussion about legal proceedings or outcomes;

4. Do not talk politics;

5. Do not post personal or protectively marked information;

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

7. Do not use personal devices to post from PSNI accounts;

8. Do not compromise operational activities;

9. All posts must be in the public interest. Do not promote personal activities, interests or preferences, and;

10. Use common sense and plain English

Appendix B Social Media Appropriate Guidance

i. No offensive posts;

ii. No Political posts;

iii. No religious posts;

iv. No swearing;

v. No comments relating to 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, accusatory or incite criminal activity will be deleted. The PSNI is not responsible for content posted up by members of the public.