SERVICE INFORMATION SYSTEM	
Title	**Social Media**
Category	**Administration**
Number	**A45**
Status	**v3.0**
Action	**By all Northamptonshire Fire and Rescue Service (NFRS) and Northamptonshire Police personnel**
Accountability	**Assistant Chief Fire Officer (ACFO) - Corporate Services**
Security classification	**Official**
Executive summary	This policy outlines the use of social media in the workplace but also to makes clear staff responsibilities as employees of the Northamptonshire Commissioner Fire and Rescue Authority (NCFRA) when engaging and publishing through social media whether at work or in their own time.

Contents

Job title	**ACFO – Corporate Services**
Date	**30 August 2019**
Review due	**30 August 2021**

1 INTRODUCTION

This document outlines social media use and the process for setting up new accounts. It applies to all officers and staff using social media to represent either/both organisations.

The purpose of this policy is to ensure that all NFRS/Northamptonshire Police personnel recognise the importance of new and emerging media platforms for communicating with the public, whilst engaging in these new methods of communication in a responsible, co-ordinated and consistent manner.

This policy will also help ensure that when engaging in social media activity outside of the workplace (personal use of social media), all staff act in a way which reflects the values and reputation of the organisations.

This document is therefore designed to educate employees on how to utilise social media sites in accordance with the law, NFRS, NCFRA and Northamptonshire Police guidelines.

1.1 Ethics – NFRS

Anyone employed by or volunteering for NFRS should abide by NFRS Service Values and by policy A6 - Code of Conduct.

Guidelines on the usage and publishing on social media websites can be found on FirePlace > Service Information System > Service Information > Guidance Notes > NFRS and NCFRA Social Media Protocol.

1.2 Ethics – Northamptonshire Police

Anyone employed by or volunteering for Northamptonshire Police using social media for work purposes should ensure posts comply with the College of Policing's Code of Ethics (full version is available on Forcenet).

This states that you:

- Ensure nothing you publish online can reasonably be perceived by the public or your policing colleagues to be discriminatory, abusive, oppressive, harassing, bullying, victimising, offensive or otherwise incompatible with policing principles.
- That you do not publish online or elsewhere, or offer for publication, any material that might undermine your own reputation or that of the policing profession or might run the risk of damaging public confidence in the Police Service.

2 WHAT IS SOCIAL MEDIA?

Social media has transformed the way people interact and consume information. Traditional publishing methods have shifted to an interactive model where everyone can be a publisher of content and where there is a far greater level of interaction and engagement between publishers and users. It has also made it possible to reach and target a demographic traditionally harder to reach and engage with.

It should be used as a platform to re-enforce the core priorities of the organisations and is an effective tool to engage with communities, identify concerns and emerging issues, and gather intelligence and issue news releases

and appeals for information. It is also an effective way to show the 'human' side of the emergency services.

NFRS and Northamptonshire Police have accounts on social media platforms; including Twitter, Facebook, YouTube, LinkedIn and Instagram etc.

These all draw in content from both organisations' websites:
www.northantsfire.gov.uk
www.northants.police.uk

2.1 What are the risks?

The main risks of using social media as an organisation are the potential damage to reputation due to misuse. If practice is not carefully monitored and assessed, incidences of misinformation could occur or unsuitable content could find its way onto web pages representative of the organisation. Misuse could be willful, through posting of defamatory or abusive content, or could take the form of inappropriate comments or conversations, whether intentional or not.

Social media must be used for the right reasons – not as an effort to be seen to be using popular media tools without fully understanding the potential risks that come with using social media.

To avoid major mistakes and turning a well meant social media experiment into a reputational disaster, it is important that we manage any potential risks through a common-sense approach and framework as well as proactively monitoring the development of such applications.

3 RESPONSIBILITIES WITHIN NFRS

The **Chief Fire Officer (CFO)** is ultimately responsible for the Service's policy on social media and for authorising any significant deviation from policy.

The **ACFO – Corporate Services** has accountability and responsibility for the overall governance of the policy and for monitoring the application throughout the organisation.

Fire Control and the Corporate Communications Team have the responsibility for posting all incident updates through the NFRS Twitter site on behalf of the organisation.

This is to ensure all content posted online is consistent with the organisation's core messages and that it does not conflict with incident information already being communicated across traditional media platforms (see appendix A: NFRS guidance on releasing operational information).

The Corporate Communications Team (Northamptonshire Police) are responsible for creating accounts, fire safety messages, assisting with post content and relevant imagery, dates of events/open days/diversity activities. They are also responsible for links to recent press releases on request from senior management.

They are responsible for creating Facebook station pages, editing social media content to ensure it meets internet content standards (where necessary). They are able to remove posts/block users, where this is possible, when seen to be appropriate and also when specific instruction has been received from a Principal

Officer (PO) or Service Information Manager. The Service Information Team (SIT) and the Corporate Communications Team respond to complaints/compliments in accordance with Service policy A18 – Customer Interaction.

The Community Protection Team may use social media platforms for investigatory purposes, in such instances individuals will comply with relevant guidance and legislation.

Jump Media Group as commissioned by the Office of the Police, Fire and Crime Commissioner (OPFCC) are responsible for resolving technical issues with the website: www.northantsfire.gov.uk

The Corporate Communications Team (Northamptonshire Police) are responsible for providing advice and guidance on issues regarding social media..

Line managers are responsible for raising staff awareness of this policy, handling any issues raised by their staff concerning this policy and for monitoring the application of the policy across their areas of responsibility. They are also responsible for approving content uploaded by their department.

All staff are responsible for adhering to this policy

4 TERMS AND DEFINITIONS

Social media – any online network or platform which requires a dedicated account and encourages public comment and interaction.

Twitter – microblogging site designed to deliver brief, bite-sized updates and messages using no more than 140 characters to people who follow your account.

Facebook – social network intended to share messages, photos and videos with friends and/or groups.

Facebook workspace - a collaborative platform run by Facebook Inc. It may be used to communicate via groups, to chat with colleagues and offers the social networks features in a corporate environment.

YouTube – video sharing site which allows users to publish and share their content.

LinkedIn – business-oriented social network mainly used for professional networking and to publicise employment vacancies.

Instagram – mobile photo-sharing, video-sharing and social networking service (not applicable to NFRS).

Periscope - live video streaming application by Twitter (not applicable to NFRS).

5 SOCIAL MEDIA ACCOUNTS

5.1 Facebook and Twitter

Facebook pages:	Twitter usernames:
www.facebook.com/northantsfire	@Northantsfire
www.facebook.com/northantspolice	@NFRSFireDogs
	@Northantspolice

The Corporate Communications Team are responsible for co-ordinating content across all organisational sites. SIT maintain an oversight and password management of the NFRS Facebook and Twitter pages.

All social media accounts are used to share news articles, promote discussion, consult with and respond to enquiries from the public (where appropriate), provide prevention information and to promote the work of both organisations.

Fire Control have access to the NFRS Twitter page to be able to monitor/manage urgent out of hours queries following contact with the Officer Of the Day (OOD) for advice and direction.

A number of Police staff have access to Northamptonshire Police's page in order to manage out-of-hours queries and respond to incidents which do not meet the threshold of contacting the on-call press officer but require publication.

Requests for new pages/accounts not mentioned above may be considered (see section 6). Site administrators/account holders are responsible for the ownership and operation of their social media pages i.e. uploaded posts and responses where possible.

The 'banner' image at the top of both respective pages will be used to publicise ongoing campaigns or events. Requests for this to be changed will be considered and should be emailed to: news@northants.pnn.police.uk.

All NFRS employees need to make themselves familiar with the NFRS and NCFRA Social Media Protocol published on FirePlace.

5.2 Facebook Workplace

A collaborative platform run by Facebook Inc. It may be used to communicate via groups, to chat with colleagues and offers the social networks features in a corporate environment.

5.3 LinkedIn – Northamptonshire Police

www.linkedin.com/company/northamptonshire-police-force

Northamptonshire Police has a LinkedIn account which is used to promote employment vacancies within the organisation and ownership sits with the Corporate Communications Team.

Requests for items to be posted to the account should be emailed to: news@northants.pnn.police.uk.

NFRS do not currently hold a LinkedIn account.

5.4 YouTube

www.youtube.com/northantspolice and www.youtube.com/northantsfire

YouTube is used by Northamptonshire Police and NFRS to host videos produced by the Force and the Fire Service. Ownership of the accounts sit with the Corporate Communications Team. The account is also monitored for inappropriate or offensive language which can be removed if required.

5.5 Instagram – Northamptonshire Police

www.instagram.com/NorthamptonshirePolice

Northamptonshire Police's corporate Instagram account is currently predominately used to promote ongoing campaigns. Ownership of the account sits with the Corporate Communications Team. The account is also monitored for inappropriate or offensive language which can be removed if required.

5.6 Periscope – Northamptonshire Police

Periscope is used to live broadcast press conferences and launches. A selected number of officers are part of a trial for wider use across Northamptonshire Police.

Periscope must not be used without prior authorisation of the News and Publishing Team.

6 REQUESTING A NEW SOCIAL MEDIA ACCOUNT

Requests for social media accounts or access to an existing account will be considered and the following procedures must be followed.

New account requests

1. Email the Corporate Communications Team at news@northants.pnn.police.uk outlining what type of social media account is required, including your role/position and an outline of how you intend to use it.
2. The Corporate Communications Team will review the request and either email or speak to you directly.
3. If approved, accounts will be set up by the Corporate Communications Team, branding applied and where necessary linked to existing accounts and lists. If an account is refused, a reason will be provided as to why.
4. The Corporate Communications Team will provide a username and password which must not be changed without authorisation. The password must not be disclosed to anyone other than a member of the Corporate Communications Team.
5. The user will be required to undertake a mandatory training session prior to the account being used, regardless of existing skill base.

7 ACCOUNT USAGE

7.1 NFRS accounts

There is an expectation accounts will be regularly used. Using social media should not detract from day to day work. Equally it will only be affective if used

on a frequent basis. There is no minimum or maximum number of posts or instances when they should be used.

A cross promotion of posts is encouraged at all times. This will include for instance sharing videos from YouTube on Facebook and Twitter accounts.

7.2 Northamptonshire Police accounts

If a social media account is approved, there is an expectation it will be regularly used. There is no minimum or maximum number of posts/updates or instances when it should be used.

Social media usage should not detract from your day to day work. Equally, it will only be effective if used on a frequent basis.

Accounts will be monitored for usage and content as well as inappropriate posts or updates. If an account is being used inappropriately, posts/updates may be removed and the individual contacted and guidance offered (refer to section 15 for more details).

Remember, posts are public. They will be shared by not only other approved users of social media from the organisation(s) but also by members of the public.

8 ACCOUNT REMOVAL

Accounts will be closed if requested, if deemed necessary or after a period of inactivity.
The Corporate Communications Team will monitor approved accounts for inactivity. If previously approved accounts are not being used, the user will be contacted and guidance offered.

The Corporate Communications Team will seek to close accounts which have not been used for 60 days, unless mitigating reasons such as prolonged absence can be provided.

9 LANGUAGE AND STYLE

Formal tone and language is not appropriate on social media and should be avoided. Aim for a relaxed, conversational style. Content should remain professional but avoid jargon, acronyms and 'corporate speak'.

Content should be concise and to the point. Do NOT emulate 'youth speak' as it can come across as patronising.

For more general guidance on how to interact on social media go to FirePlace > Service Information System > Service Information > Guidance Notes > NFRS and NCFRA Social Media Protocol.

10 POSTING ON BEHALF OF NFRS/NORTHAMPTONSHIRE POLICE

Group accounts: These should only be used to post information directly relating to the work of the organisation. Be professional and give information about campaigns, events and the activities of the department/group.

Individual accounts: Users with individual accounts may post non work-related content. However, the user is reminded the primary purpose of the account is to

highlight their role within the organisation and this should remain the core content of the account.

Personal posts should not bring yourself or the organisation into disrepute. Careful consideration should also be given to the disclosure of personal information and location based data.

Hashtags: (#) The # function allows users to 'highlight' a word(s) to allow easy aggregation of a topic. These should be used when mentioning geographic locations (e.g. towns and villages) or as part of an ongoing campaign to aggravate content.

Photos: Can be posted where appropriate. As with words, remain professional and do not post any photos which would compromise ongoing activities or investigations or bring the organisation or yourself into disrepute.

Photos with a small number of people in should not be posted without obtaining their consent. (This would not apply to large public events e.g. football crowds or a wide picture of a busy park on summers day).

Do not identify offenders or victims in photographs.

Police should contact the Corporate Communications Team for further guidance on photo use. NFRS employees should adhere to Service policy B28 - Digital Imagery for use of service images.

Use common sense. Think before you post. If in doubt, don't post.

Links: avoid using long URL links in your post. If you are going to include a link in a post, use a URL shortening service such as Bitly (https://bitly.com). This looks smarter and will save you characters.

This policy should be read in conjunction with the guidance note on the Responsible Use of Social Media.

10.1 Responding to questions and messages

Accounts should be regularly checked for questions and/or direct messages. Questions should be answered accordingly or the individual signposted to the correct department/contact (NFRS see Standard Responses for Social Media).

Members of the public should be reminded not to report incidents via social accounts and should use 101 or 999. However, it is acknowledged this may still happen. If this happens, the owner or moderator of the account in question should use their judgement as to whether the post needs to be replied to or forwarded accordingly.

Compliments and complaints on all NFRS pages are logged by the SIT into the Workflow system and dealt with in accordance with Service policy A18 – Customer Interaction.

10.2 Promoting your organisations' social media accounts

Promoting social media accounts is key in order to reach as many communities as possible. This allows for a wider audience of various safety messages and campaigns, warnings of incidents or the promotion of events.

Guidance on how to promote your social media can be found on FirePlace > Service Information System > Service Information > Guidance Notes > Promoting Social Media Links.

10.3 What not to post

Do not divulge sensitive information or anything which will compromise ongoing investigations or operations. This applies to both words and images.

E.g.: "*About to go out on a drugs raid. Part of a big operation across #Northampton this morning*."

Accounts will be followed by members of the media as well as members of the public. Do not divulge information which has not been approved for release. The Corporate Communications Team will be expected to lead on certain events/ announcements via the corporate account

If contacted through social media by a member of the media to provide an official comment or statement, refer the individual to the Corporate Communications Team.
Do not divulge personal information that may identify your family or where you live.

Do not 'chat' among colleagues in the same post/update/thread. Use email or phones to discuss things with other staff members.

Do not post personal information or anything that identifies someone or their property without consent.

Do not post anything potentially defamatory.

Judges tell juries a statement about a person is defamatory if it 'tends' to do any one of the following:

- Exposes an individual to ridicule, hatred or contempt
- Causes an individual to be shunned or avoided
- Lowers an individual in the estimation of right-thinking members of society, or
- Disparages an individual in their trade, office or profession

For more guidance see appendix A - NFRS Guidance on Releasing Operational Information and go to FirePlace > Service Information System > Service Information > Guidance Notes > NFRS and NCFRA Social Media Protocol.

10.4 Key social media guidelines

1. Think before you post and if in doubt, don't
2. Don't post in anger or under the influence of alcohol
3. Don't compromise operational activities
4. Use common sense, standard English and no jargon
5. Promote the work of your organisation
6. Don't post irrelevant photos
7. Never share your password
8. Reply to direct questions promptly and respectfully
9. Don't criticise a judge's sentencing
10. Be careful of 'talking politics'

11 PERSONAL USE OF SOCIAL MEDIA

NFRS/Northamptonshire Police's reputation for quality and service in the community is crucial and the public must be able to trust the integrity of all our staff.

Therefore, when identifying themselves as an NFRS employee, discussing the organisation, or discussing individual members of staff, all employees must:

- Not engage in activities on the internet which might bring the organisation into disrepute
- Never use social media to intimidate, bully or in any way attack or abuse colleagues or members of the community
- Not post derogatory or offensive comments on the internet
- Act in a transparent manner and make it clear that any views and content are personal
- No images taken in the process of carrying out your work duties to be posted on personal social media accounts; refer to policy B28 – Digital Imagery for use of service images

Social media content which does not identify the individual as an NFRS employee, does not discuss the organisation or individuals who work for NFRS, and is purely about personal matters, would normally fall outside this guidance unless another NFRS policy was breached.

11.1 Hand held technology (smart phones, tablets etc.)

Hand held technology has created new and evolving ways of accessing social media tools, meaning employees may have greater access to these sites. Employees are reminded that the guidance contained in this policy applies to all forms of social media, regardless of whether they are accessed from a work computer, personal computer or a mobile phone.

11.2 Privacy

Employees are reminded, in general, to check their privacy settings on social media sites to ensure they are not compromising either their personal security or the security of NFRS/Northamptonshire Police. Remember, these websites are accessible by anyone online and the content a user chooses to put on there is at their own risk.

Certain social media sites, including Facebook and LinkedIn, allow users to formally identify themselves as employees of an organisation. Users should carefully consider the risk of doing this.

Publically visible personal social media accounts may be monitored by members of the media and other members of the public.

Association of Chief Police Officers (ACPO) guidance recommends that Northamptonshire Police personnel do not declare their employment status with a Police Force.

NFRS personnel should consider all risks associated with declaring employment status on publicly visible accounts.

Careful consideration should also be given to uploading/sharing images which show any individual in a NFRS/Police uniform or clothing which identifies them

as working for the organisation. Users who opt to share such images should ensure these are not publicly viewable and that careful consideration has been given to who among their personal network/friend list can view the images.

12 LOCATION BASED TRACKING

Most modern social media applications and services will provide a geotagging option to link a status update, post, photo or video to a location. This can be as detailed as position in a street.

Ensure location based services do not compromise operational locations or personal information. Turning this service on or off varies depending on the handset or computer being used. Further guidance is available from the Corporate Communications Team.

For advice on location based tracking on devices supplied to NFRS personnel submit an IT request via Workflow.

13 SOCIAL MODERATION

Social media accounts are monitored for inappropriate comments and replies.

Accounts are monitored during office hours by the Corporate Communications Team. Limited moderation will take place out of office hours by a member of the Corporate Communications Team if they are aware of a 'post' which may require attention.

Facebook has a 'profanity' filter. This should prevent offensive language from being posted. Additional words and names can be added and removed as required. To request the addition of a name or phrase, email news@northants.pnn.police.uk.

When inappropriate, offensive, defamatory, intimidating or threatening comments are made, the following actions/procedure should be taken.

1. Using the Snipping Tool  on your computer (found in Start > All Programs > Accessories > Snipping Tool) cut out the comment and paste it into a new email. Alternatively, you can use the Print Screen button  (usually located next to the F12 key) on your keyboard and paste the image into the email. Send emails t: news@northants.pnn.police.uk.
   If viewing on a smartphone, use the 'capture screen' function of your device. This differs between handsets, but on iPhones this is done by pressing the 'home' button and 'power' button at the same time. This will save the image to your default photo gallery.

2. The offending post should be 'hidden' from public view if the social media platform allows. If not, it should be removed.

3. A warning will be provided to either the individual user or wider user base by the Corporate Communications Team.

4. If similar posts by the same individual persist, the Corporate Communications Team will ban users from the social network in question.

Please refer to the flow chart (appendix B) for guidance on how and when it is appropriate to respond to comments.

14 DATA PROTECTION ACT

The Data Protection Act 2018 contains eight Data Protection Principles. These specify that personal data must be:

1. Processed fairly and lawfully
2. Obtained for specified and lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept any longer than necessary
6. Processed in accordance with the 'data subject's' (the individual's) rights
7. Securely kept
8. Not transferred to any other country without adequate protection in situ

Full guidance on Data Protection can be found on the Information Commissioner's Office website – Guide to Data Protection.

15 COMPLIANCE

All employees are required to abide by this policy. If inappropriate content is posted on a work social media account, the Corporate Communications Team will ask for it to be removed or remove it. The individual may be reported to their line manager and or become subject to disciplinary procedures as appropriate. Accounts may be frozen and/or removed by the Corporate Communications Team.

15.1 Northamptonshire Police non-compliance procedure

If inappropriate content is posted on a force social network by an employee of Northamptonshire Police or an employee of the OPFCC, the Corporate Communications Team will ask for it to be removed or remove it. The individual may be reported to their line manager or Professional Standards Department (PSD) as appropriate.

15.2 NFRS non-compliance procedure

Employees whose use of social media, if found to be in contravention of this policy, may be subject to disciplinary action in accordance with service policies A23 – Disciplinary Procedure for Grey Book including Fire Control and Fire Staff.

16 RELATED POLICIES AND GUIDANCE

- Freedom of Information Act 2000
- General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Defamation Act 1996
- Contempt of Court Act 1981
- Human Rights Act 1998
- European Convention on Human Rights 2000
- Service policy A18 – Customer Interaction
- Service policies A23 – Disciplinary Procedure
- Service policy B28 – Digital Imagery
- Guidance note Standard Responses for Social Media
- Guidance note Promoting Social Media Links
- Guidance note Responsible Use of Social Media
- Guidance note NFRS and NCFRA Social Media Protocol
- NFRS Facebook template
- NFRS Twitter template

NFRS GUIDANCE ON RELEASING OPERATIONAL INFORMATION

Information released to the media at the scene of an incident which the fire and rescue service are taking the lead responsibility, should only be provided by the Incident Commander (IC), Media Liaison Officer, Gold Commander or a person delegated by the IC or Gold Commander. The following applies to this type of incident or via Fire Control when they publish the twitter feed.

Information that can be released:

- Gender of individual(s)
- Date and time of incident
- Times of call, attendance, stop and return
- Location – street name and area
- Stations that appliances attended from
- Number of personnel attending
- General description of incident (see exceptions below)
- Details of actions e.g. appliances and apparatus used
- Number of people rescued and how
- Type of building – general e.g. semi-detached house, disused warehouse
- Associated safety message (as confirmed by the Prevention. Safeguarding and Partnerships Manager)
- Positive action taken by NFRS personnel

Information that should not be released:

- Names, or any reference which would identify casualties or fatalities
- House number of a domestic property
- Name and/or location of commercially sensitive premises
- Information relating to cause of death
- Information relating to incidents in central government establishments such as prisons
- Specific information regarding fire and rescue personnel or vehicles
- Suspected medical conditions of people – enquiries should be referred to the ambulance service and/or police
- Information concerning an explosive or incendiary device
- Any assumption
- Any sensitive details which may embarrass or upset someone

A ‘no comment’ response should not be given as this can encourage mistrust or doubt. It is better to give some information so the media and public have a general comment.

Where another agency has taken the lead responsibility or off site Silver or Gold Command is operating, the lead agency will manage the release of information, and will advise on the information that can be released by NFRS.

Dealing with the media

When dealing with the media (in accordance with media training) it is important to remember that you are representing and speaking on behalf of NFRS, it is therefore necessary to retain a professional and courteous manner. A negative or inaccurate report to or in the media can damage the reputation of the Service and cause confusion.

You will confirm with the interviewer prior to commencement of any interview the areas to be covered and declare areas you will not cover within the context of the interviewer; or, areas likely to try to illicit a response to any current media area.

You are recommended to:	**You are not recommended to:**
Keep the media informed of what is happening and tell them when you are likely to have any further updates	Make any comment which is not factual or based on supposition or assumption
Deal with any enquiries as quickly as possible	Use the phrase 'no comment'
Ensure information is timely and relevant	Comment on a subject that is outside your responsibility
Be sure of any facts before referencing them	Use statistics or performance information which has not been verified for release
If you feel you have been misinterpreted ask them to repeat back to you the information they have taken	Criticise another service or organisation
Clarify if an interview is live or recorded	Talk off the record
Clarify current safety advice	Indicate the cause of a fire if there is an investigation underway

APPENDIX B

PROCEDURE FOR RESPONDING TO COMMENTS ON SOCIAL MEDIA SITES