NORTHAMPTONSHIRE FIRE AND RESCUE SERVICE

Social Media Policy

SERVICE INFORMATION SYSTEM	
Title	**Social Media Policy**
Category	**Administration**
Number	**A45**
Status	**V5.0**
Action	**By all Northamptonshire Fire and Rescue Service**
Accountability	**Communications**
Security classification	**Official**
Approval by PO	**ACO Enabling Services**
Approval date	**29 July 2025**
Published date	**29 July 2025**
Review date	**29 July 2027**
Executive summary	This policy outlines the use of social media in the workplace and makes clear staff responsibilities as employees, cadets or volunteers with the Northamptonshire Commissioner Fire and Rescue Authority (NCFRA) when engaging and publishing through social media whether at work or in their own time.

Contents

1 INTRODUCTION

This document outlines social media use and the process for setting up new official NFRS accounts. It applies to all firefighters, staff, volunteers and cadets using social media to represent Northamptonshire Fire and Rescue Service (NFRS).

We are Northamptonshire Fire and Rescue Service and we want to use social media to enhance and maintain our reputation as a fire service of quality, that works hard to keep the people of Northamptonshire safe.

Our corporate social media accounts (currently X, Facebook, Instagram, YouTube, Threads, Next Door and LinkedIn) are great ways to communicate with the public and promote the organisation and the good work it does, to engage with a wide audience across the county and to make us an employer that people would aspire to work for, in the many different roles we undertake. If our use of social media goes wrong, it has the potential to seriously damage our reputation. We must ensure that our use of social media not only reflects with credit on the values of NFRS, but that it also delivers us appropriate business benefits for the time put in.

If you are using a NFRS social media account, you are representing our service when you post. The purpose of this policy is to ensure that all NFRS personnel using official social media channels are authorised and communication takes place in a professional, consistent and coordinated manner. This policy gives guidance on the standards expected and the behaviours that must be applied by anyone using official NFRS social media channels. It is intended to support you to show our service in the best possible light and not to unintentionally cause offence. Every care must be taken to avoid the publication of misinformation, causing of offence or prejudice to an individual, business or other organisation.

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 organisation's corporate channels.

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 organisation.

In the event of any misuse of NFRS social media channels, disciplinary policies will apply.

2 ETHICS

Anyone employed by, or volunteering for NFRS should abide by the Fire Core Code of Ethics.

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 joint Fire and OPFCC Communications Team are responsible for policy and strategy, which is carried out on a day-to-day basis by the Senior Social Media Engagement Officer.

All members of the joint Fire and OPFCC Communications Team have access to the corporate social media accounts, where details are centrally held, and monitor these in the absence of the Senior Social Media Engagement Officer. The Joint Communications Team has responsibility for posting updates and content on the main NFRS Facebook, X (previously known as Twitter), Instagram, LinkedIn, Nextdoor, Threads and YouTube channels. They also have access to share posts on the station accounts when needed. These

channels can change accordingly to align with Communication strategies and as platforms evolve and develop.

Out of office hours - Fire Control can post to social media where the incidents don't meet the criteria for calling the on-call communications officer (who is a member of the Northamptonshire Police Corporate Communications Team) to post incident updates to warn and inform the public.

The Senior Social Media Engagement Officer is also responsible for creating new social media accounts and pages and editing social media content to ensure it meets internet content standards (where necessary). They can remove posts/block users, and revoke access where this is possible, when seen to be appropriate.

The Office of the Police Fire Commissioner Customer Service Team will respond to complaints/compliments passed to them in accordance with Policy. 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 REQUESTING A NEW CORPORATE SOCIAL MEDIA ACCOUNT

Requests for new corporate social media accounts or access to an existing account will be considered by the Fire Communications Team, however in general, it is always better for messaging to go out on the main corporate accounts, which is where our greatest audience sits and engagement can be developed.

Before permission is granted, this policy will need to be read and acknowledged.

Requests can be emailed to FireNews@northantspfcc.gov.uk detailing what type of social media account is required or which account you would like access to, including your position and an outline of how you intend to use it.

- Fire Communications Team will review the request and either send a return email or speak to you directly
- If you haven't used the social media channel before, you will be expected to attend some training before being approved, and you will be required to read the relevant social media guidance
- Once approved, the account will be set up by the Fire Communications Team
- Fire Communications Team will, where applicable, set a password for your account and let you know what it is - if you change this for any reason, you must inform the team immediately so they can update your password which is kept in a secure folder
- Passwords must not be disclosed to anyone other than the Fire Communications Team and your account should not be used by anyone else to post on your behalf
- Fire Communications Team will maintain a list of the official social media accounts authorised by the Service

4.1 Account Names

Official social media usernames are to be named based on the role, the team or the area the account represents. Fire Communications Team can assist with the most appropriate username so that there is consistency across the organisation. All accounts must be easily identified as being part of Northamptonshire Fire & Rescue Service network, this includes relevant descriptions and correct use of service branding.

5 SOCIAL MEDIA ACCOUNT USAGE

If a social media account is approved, there is an expectation that the account holder will update the account regularly and monitor comments and messages.

Social media usage should **not** detract from day-to-day work. Equally, it will only be effective if used frequently. Accounts can be closed if they have not been usedfor 60 days unless appropriate mitigation can be provided.

You can email or call the Fire Communications Team for guidance and support at any time during working hours, and out of hours, **in an emergency**, the police on-call communications officer (via Control).

Always remember, the media follow all our accounts and anything you post is in the public domain and can be quickly picked up and reported. Please do tell the Fire Communications Team about any posts so that they can deal with any follow-up media enquiries quickly and professionally.

Please remember that anything you 'like' from social media accounts can be seen.

5.1 What to post

Before you post – ask yourself if people can use the information to help keep themselves safe? Is the post promoting the reputation of our fire service? Keep the people involved at the front of your mind – colleagues or a member of the public: how would you feel if it was about you?

If you decide to post, keep it short and factual and make sure your post is saying something people will understand in jargon free language. Acronyms should be explained.

There is plenty of scope to use photos and video and make great content but stick to these dos and don'ts:

Don't

- Don't post names – even of colleagues unless you have their **express** permission
- If posting about an incident, do not include the full address or any details that could lead to the identification of individuals or properties involved. Posts should focus on public safety and awareness—link to relevant prevention messages where appropriate. Always notify the Fire Communications Team when posting so they can respond to media interest or enquiries. There is no requirement to post about every incident, and doing so as a running log is discouraged.
- Don't post pictures that can identify a property, or personal property inside a house unless you have the owner's clear permission. When asking permission to use photographs, ensure they understand how the photographs will be used
- Don't post about businesses or allegedly dangerous products without clearance
- Please don't repost content without checking it is current and accurate and from a credible source. Don't repost content from individuals as their previous social media content may not align with our values.
- Social Media accounts should not be used to mention, promote or endorse any business or union without express approval from the Fire Communications Team Requests for charitable donations and promotion of charities should only be shared if they are for our corporate charity – the Fire Fighter's Charity
- When engaging online, do not post any confidential, internal-use only or copyrighted information that belongs to NFRS or third parties without written permission. Information to be protected includes music, videos, text, graphics, newspaper cuttings/screenshots and photographs
- Do not make statements about NFRS performance or corporate affairs

or post content that is strategic or confidential information. Refer any Freedom of Information (FOI) requests to Information Assurance Unit, Enabling Services

- Don't use social media to have conversations with colleagues or air complaints
- Don't use corporate accounts to share details of your personal life

Do

- Make sure posts, including those with images and videos are accessible. Videos must be shared with subtitles and voice over as much as possible. Photographs and graphics **must** have ALT text where platforms allow. Guidance around accessibility can be obtained from the Fire Corporate Communications Team
- Think before you post - will the person involved in the incident or event be happy that you have posted? Is there a clear purpose to posting?
- Be nice
- Be careful - posting on social media is the same in law as publishing in a newspaper, for example and it is very difficult to delete completely
- Post great pictures and videos that showcase our work. At an incident, you may use pictures taken from a public place like the pavement. Try to avoid any vehicle registration numbers or faces of people not involved.
- Ask – would you feel comfortable seeing this in a newspaper?
- Get the permission of someone you are posting about
- Think about the external context when posting. For example, during a sensitive period, images of fun quizzes or overuse of emojis would be inappropriate
- Take part in messaging in coordinated way if requested by Fire Communications Team (example around a water safety campaign, or other themes)

If in doubt, please contact the Fire Communications Team who will also

be able to help you use your content and ideas to reach your community in lots of different ways. You can call us on 101 extension 342408 or email FireNews@northantspfcc.gov.uk

The Fire Communications Team is responsible for monitoring and creating content for the primary, 'Northamptonshire Fire' branded accounts (Facebook, X, Instagram, LinkedIn, Next Door and YouTube).

Other accounts within the NFRS network will be monitored adhoc during office hours by the Fire Communications Team, for usage and to ensure only appropriate content is being published. Limited moderation will take place out-of-office hours by a member of the Communications Team if they are aware of a 'post' which may require attention. However, the team are not responsible for replying to any comments, issues or complaints as the responsibility lies with the content owner/creator or account admin. If you create content and upload to an official account, you will need to monitor for engagement and reply accordingly from the official Station/department account.

If an account is used inappropriately, posts will be removed, the individual will be contacted and guidance from the Fire Communications Team will be offered. Access can be revoked by the Senior Social Media Engagement Officer if policy is breached.

If you see comments or inaccuracies, please contact the Fire Communications Team offline.

Direct Messaging through social media is not part of the NFRS communications strategy. The facility to send or receive Direct Messages on Station Facebook accounts is turned off to ensure members of the public contact the stations in the appropriate way (email or phone call to the Service Information Team). This is to enable advice given is consistent and communications to be open and transparent to offer protection to both staff and members of the public.

If you move stations, leave the organisation or no longer require or need access to the account, please inform the Fire Communications Team.

5.2 Managing an account during a crisis

In certain situations, for example, after a death in Service, a major incident or if there is a large amount of media attention on the Service, you may be asked to postpone any social media posts planned for your account.
Any requests to postpone content must be complied with. If you are asked to comment on a confidential or crisis-situation then please refer people to the Fire Communications Team.

6 POSTING PHOTOGRAPHS

When posting photos as part of your social media posts, please consider the following:

- As with words, photos must remain professional and not compromise ongoing activities or investigations or bring the organisation or yourself into disrepute
- Always get consent for photos you take that feature people. Photos featuring individuals or small groups must not be posted on social media without their consent. For large groups of people, consent is not required – e.g. fans attending football games or a photo of a busy town centre or street. Any photos that are going to be used for any marketing campaigns or for public use, always gain consent and let them know exactly where they will be used
- Photos of anyone under 18 should not be used without parent or guardian consent - if in doubt of any photo, ask for consent to share and tell them exactly where it will be shared
- If your photos include colleagues, you must check they are happy for you to share on social media before you publish - also be mindful about who is in the background of your photos
- Think not only about what is in the foreground of your photo, but

whether there is any restricted information shown in the background

- You should not post, or digitally manipulate images, you are not the copyright holder of or do not have permission to use
- The use of AI-generated images that depict or imply real-life scenes must not occur without explicit approval from the Fire Communications Team. These images, while visually convincing, can easily mislead audiences and blur the line between reality and fabrication. Using them without proper oversight risks spreading misinformation and may seriously undermine public trust in our communications. Misuse could call into question the integrity and credibility of our organisation.

Remember photographs posted on social media may be picked up and used by anyone and could be re-used in a context that the person posting or those pictured intended.

Use common sense, think before you post and always seek permission. Contact Fire Communications Team for further guidance on photo use.

7 PERSONAL USE OF SOCIAL MEDIA

NFRS'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, members of the community or organisations
- 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

- Remember that what you ‘like’ and ‘share’ reflects on you. Liking or associating yourself with social media sites and content that is inappropriate could compromise you and, if you have identified yourself as working for NFRS or it is obvious from your posts that you are an employee of the Service, then it reflects on the professionalism of the Service too
- Not to use the Northamptonshire Fire & Rescue Service logo or images, as your avatar/photo identifier. This is the image that is seen on social media by all - regardless of your account settings to identify who you are. This is so the public aren’t confused thinking it is an official NFRS account rather than a personal one.

While sharing the messages that have been published on the main NFRS accounts or station pages onto your own personal accounts is welcomed, please do not post the information directly to your own social media accounts, as though it is an official post. eg, job adverts, prevention advice or events. These should come from an official page – best practice is to share or repost from the main posts.

8 USE OF DIRECT MESSAGING APPLICATIONS

Applications such as WhatsApp, Messenger, Signal and Telegram allow users to send direct messages individually or to groups and are widely used by many people.

There have been a number of high-profile misuses of WhatsApp and other instant messaging applications across the public sector.

It is acknowledged that WhatsApp is in widespread use for social networking, and people socialise with work colleagues. It is also acknowledged that NFRS utilise WhatsApp for business purposes on occasions. This policy encourages that use of WhatsApp for business purposes should be kept to an absolute

minimum. There must be a clear dividing line between work related business and group chats that involve work colleagues that are not solely for progressing business objectives (i.e. for more social matters).

You should be mindful about drift between personal and business use of instant messaging services. Use of WhatsApp on business phones must always remain professional and the Service values and disciplinary policies apply to such use. Likewise, business related instant messaging on personal phones are covered by this policy.

Any data breaches carried via WhatsApp could result in disciplinary or legal proceedings.

Anyone choosing to use it is expected to take personal responsibility for complying with policy and procedure, including Information Security Policy and other Information Assurance related policies (e.g. Data Protection/GDPR, Records Management, Freedom of Information) as well as this Social Media Policy.

In 2022, the Information Commissioners Office (ICO) conducted a review into government use of private correspondence channels, including WhatsApp, following messages that were leaked by ministers and officials during the pandemic. The investigation found that the lack of clear controls and the rapid increase in the use of messaging apps and technologies, including WhatsApp, had the potential to lead to important information being lost or insecurely handled. The ICO concluded that there were real risks to transparency and accountability. Their guidance states that any official business should be conducted through corporate communication channels such as departmental email accounts, wherever possible and that official information exchanged through private channels should be transferred on to official systems as soon as possible.

Public officials should be able to show their workings through proper recording of decisions and through the Freedom of Information Act, to ensure that trust in those decisions is secured and lessons are learnt for the future.

8.1 Making informed decisions about WhatsApp use

- **Participation is voluntary**: You are not required to join any WhatsApp group for work.
- **Be aware of group members**: Your phone number and profile information are visible to all members.
- **Group admin responsibilities**: Remove members who leave and close groups when no longer needed.
- **Check privacy settings**: Adjust who can see your profile and where images are stored.
- **Data sharing risks**: WhatsApp, owned by Meta, may share data across platforms, including internationally, where UK data protection laws may not apply.
- WhatsApp security disclaimer states that the service is not warranted as secure or safe
- **Security Concerns**: WhatsApp has had past security breaches, and messages could be accessed by third parties.

8.2 Device & message security

- Be mindful of where you leave your phone and who has access to it.
- Disable message previews on your lock screen to prevent unauthorised viewing.

9 COMPLIANCE

All employees/volunteers are required to abide by this policy.
If inappropriate content is posted on a **work social media account**, the

Communications Team will ask for it to be removed or remove it. The individual may be reported to their line manager and become subject to disciplinary procedures as appropriate. Accounts may be frozen and/or removed by the Communications Team.

If you operate a **personal social media account** where you are identifiable as an employee of NFRS, either via the content you have posted or via media you have posted then you must abide by this policy. Whilst the Service is unable to mandate that you remove possibly offensive posts or ones that breach our code of ethics, you could still be subject to formal disciplinary action, which could ultimately result in dismissal.

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 policy A23 – Disciplinary Procedure (Grey Book including Fire Control) and policy A23 - Disciplinary Procedure (Fire Staff).

10 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 A12 – Anti-Bullying and Anti-Harrassment
- Service policy A18 – Customer Interaction
- Service policy A23 – Disciplinary Procedure (Grey Book)
- Service policy A23 – Disciplinary Procedure (Fire Staff)

11 DOCUMENT HISTORY

Impact assessments

An Equality Impact Assessment (EqIA) was completed on:

EqIA	29/05/2025

Audit trail

Listed below is a brief audit trail, detailing published versions of this policy:

Document control			
Version	Date	Author	Status
2.0	06/10/16	J Miles	Published
3.0	30/08/19	SIT	Published
4.0	08/06/21	SIT	Published
5.0	29/07/2025	Helen Franks (Communications)	Published

APPENDIX A

NFRS GUIDANCE ON RELEASING OPERATIONAL INFORMATION

Information released to the media at the scene of an incident which NFRS 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 –

Information that can be released:

- 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 or incidents involving our partners eg police, councils, health organisations
- 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

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. If you are not sure, please check with the Corporate Communications Team.

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.

Approaches from the media **must always be referred** to the Fire Communications Team including requests made for comments or interviews via social media platforms.

APPENDIX B

NFRS EXAMPLES OF POSTS

Here are some sample tweets you might find useful:

From Control to warn and inform

Sample posts for stations

Engagement event and visits, car wash/charity events, safety advice, recruiting on call (in agreement with recruitment manager/ Fire Communications Team). **Remember to tell the Fire Communications Team about your forthcoming events.**