



**Shropshire**  
Fire and Rescue Service

## Brigade Order

### Administration

Title	Social Media
-------	--------------

Contents	Page No.
Purpose	2
Strategic Aims	2
Introduction – What is social media	2
Appropriate Use of Social Media	4
General Data Protection Regulation	5
Do You Need A Social Media Account?	5
Use of Service equipment for social media activities	7
Monitoring Usage	8
Business contacts	8
Whistleblowing	8
Breaches of the policy	8
Legal Guidelines	9
Appendix - Personal and business do's and don'ts	

### Roles, Responsibilities and Review

The **Chief Fire Officer** is responsible for ensuring this Order is implemented across the Brigade.

The **Assistant Chief Fire Officer Corporate Services** will be responsible for the day to day operation of the Order.

The **Communications Officer** will review this Order annually or when new legislation arises, or as and when organisational needs require.

# Brigade Order: Administration

## Social Media

### Purpose

---

This Order provides information and guidance on Service requirements for the use and management of social media. The policy will help ensure that, when engaging in social media activity both for business and personal use, employees and Fire Authority Members act in a way that reflects the values and reputation of the Service.

### Strategic Aims

---

This Order supports all of the services Strategic goals as outlined in the Annual Plan.

### Introduction

---

The term 'social media' refers to the use of web-based and mobile technologies to turn communication into an interactive dialogue in a public forum.

This can be for purely social reasons, but it may also be based on shared interests in work, leisure or a general desire to communicate and share information. Social media and social networking are terms that overlap and are often interchangeable.

The Service uses social media as a warn and inform tool as well as a method of sharing prevention, recruitment and other essential messaging. All social media messaging is aligned to the Service's Core Values, Core Code of Ethics and [Workplace Charter](#). All of which are outlined in our [People Strategy](#).

Social media also provides the Service with a valuable tool to engage with its community and better understand the people it serves. This in turn allows for better, more informed decision making.

Social media sites allow users to:

- Create and maintain profiles, including biographical information and their interests and preferences
- Share files such as photographs
- Have on-line discussions
- Create blogs with updates of news or events.
- Collaborate on creating and maintaining information or knowledge, known as wikis'
- Bookmark and tag sites that may be of interest to other members

Subject to the rules contained in this policy, the use of social media sites can be used within your IPDR and to form part of your development.

### Examples

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	2 of 12

There are ten main categories of social media. This list is not exhaustive and offers a general overview of social media platforms.

- Social networks - Connect with people [Facebook](#), [X](#), [LinkedIn](#) WhatsApp
- Media sharing networks - Share photos, videos, and other media [Instagram](#), [Snapchat](#), [YouTube](#) and [Tik Tok](#).
- Discussion forums - Share news and ideas [reddit](#), [Quora](#), [Digg](#)
- Bookmarking and content curation networks - Discover, save, and share new content [Pinterest](#), [Flipboard](#)
- Consumer review networks - Find and review businesses [Yelp](#), [Zomato](#), [TripAdvisor](#)
- Blogging and publishing networks - Publish content online [Goodreads](#), [Houzz](#), [Last.fm](#) [WordPress](#), [Tumblr](#), [Medium](#)
- Interest-based networks - Share interests and hobbies
- Social shopping networks - Shop online [Polyvore](#), [Etsy](#), [Fancy](#)
- Sharing economy networks - Trade goods and services [Airbnb](#), [Uber](#), [Taskrabbit](#)
- Anonymous social networks - Communicate anonymously [Whisper](#), [Ask.fm](#), [After School](#)

The Service currently uses Facebook, X (Formerly Twitter), Instagram, Youtube and its website as its main channels for external communication. These are run by the corporate Communications Team however additional accounts for specific fire stations are in place where the crews have demonstrated they can maintain the channel.

There are other internal platforms such as Microsoft Teams, the SharePoint portal and The Pink newsletter which is run through Campaign Master.

The Service recognises that WhatsApp is a widely used communication tool within society and the Service is no exception. It should be remembered that the use of WhatsApp by members of staff should be in line with the Service's Core Values and Workplace Charter. Even on a personal device/account, may become disclosable evidence in legal hearings or public inquests.

WhatsApp is currently not a corporate tool and should not be used as a formal method of communication due to issues such as security, GDPR and FOI requests. We would encourage staff to use Teams to communicate with their colleagues.

## Implications and responsibilities

Social media is a useful tool of communications for the Service and has allowed SFRS to reach different audiences and members of the community. Many of the Service's social media channels successfully engage with thousands of members of the public, allowing for meaningful consultation and promotion of safety. They give the Service a form of two communications with the community we serve while allowing us to provide essential incident updates and safety advice.

Whilst social media is an effective way of communicating with members of the public, there are some points to be aware of with its use.

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	3 of 12

Any time someone posts on social they should have the Service's reputation in mind and be cautious not to publish anything that might damage that reputation. All employees, and those affiliated with Shropshire Fire and Rescue Service (such as contractors, agency staff etc) have a responsibility to ensure appropriate use of social media sites and be mindful of how they represent themselves on social networks. Everything posted on social media channels should be in line with the service core values and Core and Code of Ethics.

SFRS corporate communications team administrates the organisation's social media accounts, posting news on the main Facebook, Instagram and X accounts every day, sharing information from partner agencies and responding to enquiries that come in via these platforms, in conjunction with the appropriate person or departments.

Individual station accounts are managed and maintained locally by designated social media champions.

Any member of staff can make content suggestions to the corporate communications team or social media champions and they will post news, photos and events on behalf of personnel as appropriate.

Employees' use of social media can pose risks to the Service's confidential and proprietary information and reputation and can jeopardise its compliance with legal obligations.

This policy applies to the use of social media for both business and personal purposes, whether during work hours or otherwise.

It applies regardless of whether the social media is accessed using the Service's IT facilities and equipment or personal equipment belonging to members of staff or others.

Managers are responsible for taking reasonable steps to ensure that those in their teams understand this policy, and for giving guidance on the appropriate use of social media sites in the workplace and identifying social media training needs.

All employees are responsible for their own actions in the use of social media, ensuring that they read this policy and understand the content, and for seeking guidance if uncertain about how the policy impacts on both business and personal use.

Any information published online can be accessed around the world within seconds and will be publicly available for all to see.

You should remember that what you publish might be available to be read by the masses (including the Service itself, media, future employers, and social acquaintances) for a long time.

Once published, it is virtually impossible to delete all copies of information. As an employee you should take the following into consideration when using social media:

- Ensure you are aware of and comply with the contents of this document and the Code of Conduct.

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	4 of 12

- Familiarise yourself with the legal issues outlined in the 'legal guidelines' of this brigade order.
- If unsure as to whether to post any information, STOP and take advice, before making any decision to post.
- Remember that you are representing the Service, and you should avoid acting in any manner which could either bring the Service or your colleagues into disrepute.

## Appropriate Use of Social Media

---

When using social media sites, an employee's conduct may have serious consequences for the Service, other employees, members of the public, suppliers and other affiliates.

Employees should also remember that even when they are not acting on behalf of the Service, i.e. during personal use of social media, this guidance continues to apply if they can be recognised as an employee of SFRS. This includes groups where there are other members of staff present or members of the public that would be able to identify you as a member of the Service even if you have not explicitly stated so online.

If too much focus is put on using social media at the expense of other forms of publications and communications, certain groups in the community and within the organisation may feel alienated if they do not have access to, or have the relevant knowledge/skills to access, these sites. It is important to consider if social media is the most appropriate method. For the avoidance of doubt, social media should not be used for formal internal communications such as, issuing a grievance/complaint or reporting an offence. The Service has robust complaint and grievance procedures which can be found [here](#).

All members of the Service are expected to uphold SFRs values and adhere to the Core Code of Ethics and the Workplace Charter in all communications and behaviours on all social media channels regardless of who this interaction is with.

### Do's and Don'ts

Appendix A has a guide to what you should and should not post on social media for both personal and business use.

Be careful about adding applications to social media accounts as you will often be granting permission for the third-party provider to access account information and therefore may compromise the security of your account. If you use any third party apps make sure you read the small print before signing up.

Any published information must be in line with the values and standards of the Service. Examples of such include inappropriate pictures, content of a sexual nature or rude, offensive, discriminatory or bullying written text.

If one person harasses another for reasons connected to a protected characteristic; if they engage in unwanted conduct that has the purpose or effect of violating dignity; or they create an intimidating, hostile, offensive or degrading environment, it constitutes a

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	5 of 12

breach of the Equality Act 2010 and potentially a fundamental breach of contract. This applies to conduct carried out using both private phones and emails.

## **Messaging Platforms**

This policy applies to all social media and digital platforms including messaging platforms. These platforms include but are not limited to WhatsApp, SnapChat, Facebook Messenger, Telegram, Tik Tok etc. You must always act in accordance to the Service's Code of Conduct, core values and ethics.

Any breach of the Service's core code of conduct may result in disciplinary action, including but not limited to suspension, disciplinary warnings, demotion, transfer or dismissal in accordance with the [disciplinary procedure](#).

## **General Data Protection Regulation (GDPR)/Data Protection Act 2018**

Personal data, in short, means information about a particular living individual. It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

If you could identify someone from the details provided, or by combining the information provided with other information, it will still count as personal data.

The legislation is about:

- Ensuring people can trust you to use their data fairly and responsibly.
- The onus is on you to think about and justify how and why you use data.

There are mandatory modules on [LEO](#) for GDPR, please ensure you are up to speed with these. Also, there is a [GDPR area on the Portal](#) which you can access further information.

## **Do You Need An SFRS Social Media Account?**

Social media forms part of the Service's legal obligations to put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency.

The kind of information that can be posted includes:

- The general location of an incident, e.g. M5 motorway (you should not confirm house number/name or business name). Road names should only be used but you should consider whether it is necessary, adds value to the post or makes identifying an individual possible.
- Type of incident (as long as it is not considered a sensitive incident e.g. attempted suicide or bariatric rescue)
- Time and date of call/attendance
- Details of appliances dispatched
- Details of firefighting/rescue actions
- Number of rescues/injuries/extrications, subject to consideration and impact on those involved, as well as the possible future outcomes (e.g. survivability or long-term impacts on any persons, animals or pets.)
- A community safety message should always be included.

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	6 of 12

- Where appropriate, link back to the main fire service website for safety information and guidance.
- Use corporately approved images and templates which can [be found here](#).
- Use photos from incidents that show work of the Service without showing casualties or identifying features such as number plates or house numbers.
- All of the above should only be posted on SFRS accounts used for corporate use ONLY

Information that it is not acceptable to post on social media includes:

*\*Please note this list is not exhaustive*

- Names of injured persons or any persons involved without their express written permission
- Confirmation of fatalities
- Incidents that may be subject to investigations either criminal, fire safety or fire investigations.
- To imply or try to explain the incident whereby any form of blame could be apportioned, e.g. describing an RTC where one car “hit” another may imply the first car was to blame for the incident by hitting the other.
- Specific injury details
- Information or images of incidents that could possibly turn out to be fatal or where people have been seriously injured
- The names or specific ages of anyone involved in an incident, without their consent. Where necessary, refer to younger, older, youths or adults as a descriptor
- Images that could lead to the identification of a property without the resident’s consent. This includes images from within a private property.
- Information or images that could lead to the identification of any persons involved such as car registration number.
- Images with other persons in the picture (usually background) who are unaware they have been filmed.
- Images that breach copyright - do not post any information or other material e.g. a photograph of an incident, which is not generated by the Service, without the express permission of the provider.
- Any other information that is of a sensitive nature or could compromise the work of the Service. Remember that even private conversations could be subject to GDPR

Each station should have access to both a Facebook and Twitter account and have at least two dedicated users associated with the account.

Facebook accounts should include one ‘page owner’ roles for both members of the corporate communications team. At a local level, there should also be two members of staff with administrator roles.

Further editorial roles can be allocated as required following appropriate training in social media. This can be arranged by contacting the corporate communications team.

Twitter accounts are accessed by passwords and corporate communications should be notified of all these and the associate users at stations. It is the responsibility of the lead

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	7 of 12

social media champion at each station to ensure that all users have accessed training before using social media channels.

In addition, account users may be added from time to time, through approval by the CFO/ACFO organised through corporate communications.

All applications for social media accounts must be approved by the corporate communications team and staff must demonstrate:

- The account will follow the above criteria.
- The account will follow and support the organisational objectives outlined in section 2
- An understanding of responsibilities in managing the account and planned appropriate time to use it
- Full details including administration rights and email address to secure the address have been disclosed to the corporate communications team
- Approval has been sought from line managers who will monitor the content of the account
- An understanding of the service campaign calendar and how to access the resources to support them.

## **Use of Service equipment for social media activities**

---

Employees may make limited and reasonable use of Service equipment including PCs, laptops and smartphones to access social media whilst at work for non-work related activity but access should only be undertaken in an employee's own time and is subject to it not interfering with productivity.

Employees must not access any inappropriate or offensive websites and must comply with the rules under this, and associated policies

For more information, please see Brigade Order Administration 16 Part 2 Section 1 Information Technology, Policies and Procedures - Security. [Brigade Order Administration - Information Security Policy](#)

Only those with designated roles are permitted to post material on behalf of the Service. The use of Service equipment is allowed within work time although compliance with the rules under 'Implications and responsibilities' still applies.

## **Use of personal equipment for social media activities**

Employees may use personal equipment to access social media whilst at work, but access should only be undertaken in an employee's own time and is subject to it not interfering with productivity.

For more information, please see Brigade Order Administration - [Information Security Policy](#).

## **Monitoring Usage**

---

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	8 of 12



The Service reserves the right to monitor employees' use of Service internet, but will endeavour, where appropriate, to inform an affected employee when this is to happen and the reasons for it. The Service considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- Spend an excessive amount of work time accessing online content, including social media sites which interferes with productivity
- Acted in a way that is in breach of the rules set out in this policy

Abuse and misuse of the internet will be reported to the individual's line manager and may lead to disciplinary action. For example it is unacceptable to tether (hot spot) a private device to the Service internet for the purpose of personal streaming (such as Netflix, Amazon Prime etc).

For more information, please see Brigade Order Administration 16 Part 2 Section 1 – Information Technology, Policies and Procedures - Security.  
Brigade Order Administration - [Information Security Policy](#).

## **Business contacts**

---

The details of business contacts made during the course of your employment belong to Shropshire Fire and Rescue Service, including those created through professional networking sites such as LinkedIn.

## **Whistleblowing**

---

If an employee believes that this policy has been breached they should bring it to the attention of the Service in line with Brigade Order Reporting of Illegality and Malpractice – Whistleblowing.

## **Breaches of the policy**

---

Anyone can make a mistake and managers are advised to resolve any problems at the lowest level possible, as appropriate to the circumstances. If you have made a mistake or done something wrong, deal with it before it gets worse and report it to your line manager who will support you as far as they can.

Any breach of this policy will be taken seriously and may lead to disciplinary action in line with Brigade Order – Disciplinary Policies and Procedure.

Serious breaches will be regarded as gross misconduct and would include (but are not limited to) posting material which could bring the reputation of the Service into disrepute, making discriminatory or derogatory comments about colleagues, the Service, and partner agencies, or the disclosure of confidential information.

Other breaches may also be considered to be serious, depending on the circumstances including your role within the Service.

Employees must remove any material posted in breach of this policy.

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	9 of 12

Employees must co-operate to the fullest extent possible in any investigation into suspected breaches of this policy. This may include handing over any relevant passwords in situations where the Service may need these in order to investigate a suspected breach.

Employees must report to the duty group manager immediately if they see anything on a social media site that indicates a colleague may have breached this policy. The on-duty group manager will also notify the Human Resources department.

Employees can use the Service's whistleblowing procedure to raise any issues of malpractice. This is the appropriate channel for raising issues in the first instance and not via comments on social media sites.

Please refer to Brigade Order Reporting of Illegality and Malpractice – Whistleblowing.

For further information on any sections of this policy, please contact the Human Resources department.

## **Legal Guidelines**

---

In addition to the basic guidelines on posting, you should be aware of any legal issues connected with using social media.

The guidelines are intended to provide an insight into the possible complications of using social media sites while at work or for work-related purposes. They are not intended to discourage you from using social media for work purposes when necessary.

By applying the same common sense and etiquette that you apply to "real life" social situations, as well as understanding these guidelines you should avoid any complications.

The following guidelines do not constitute legal advice and are not a substitute for expert legal advice about a specific situation. Shropshire Fire and Rescue Service accepts no liability for any action taken or not taken as a result of this information.

Legal issues relating to social media

### **Defamation**

- Defamation is when an untrue statement is made about a person or company which is damaging to their reputation.
- Libel is the publication in permanent form of a defamatory statement, so the untrue statement becomes 'libel' as soon as it is recorded, e.g. in an email or posted on a website.
- It is recommended that links are only shared from reputable partners such as police, health, local authorities and approved support agencies such as Dementia UK, MORSE etc.

### **Data Protection and Freedom of Information**

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	10 of 12

- Please ensure you are familiar with the Administration - Information Legislation and Administration - GDPR [brigade orders](#) for Freedom of Information and .
- Personal information relating to colleagues, members or customers should not be disclosed via social media. Avoid providing postal addresses, phone numbers, email addresses and so on (unless they are already available on the Service's website).
- Uploading any information to social networking sites is a form of disclosure and therefore must comply with data protection principles. Information you post using social media (including the Service's SharePoint network) is subject to the Freedom of Information Act.

## Intellectual Property Rights (including copyright)

- Normal intellectual property laws apply to websites.

Staff should not do anything to jeopardise the Service's confidential information through the use of social media.

In addition, staff should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the Service as well as the individual author.

- Do not post information from private emails without permission.
- You may also commit a criminal offence by posting articles or recordings including music clips that infringe intellectual property rights. Some of these offences are punishable by custodial sentence and/or an unlimited fine.

The penalty for offences of posting infringing articles and illicit recordings respectively is a maximum fine of £5,000. This is set to increase to £50,000.

## Discrimination

- The general laws on racial hatred and discrimination on the grounds of any protected characteristic apply to the Internet.
- The Service's policies regarding bullying and harassment also apply (Code of Conduct and Dignity at Work or equivalent).
- Publishing or sending obscene material via the Internet is a criminal offence.

## Accessibility

- Where pages constitute a "service", sites are legally required to make reasonable adjustments to allow for access by people with disabilities such as blindness or poor motor control, who may be using specialist software access rather than normal browsers.
- Websites must follow the accessibility requirements for public sector bodies [available here](#)
- This is an internationally agreed recommendation for website accessibility and relevant due to the frequent links posted from the website, onto social media

Reference	Author	Status	Date	Page
Admin	CCO	Re-Written	06/23	11 of 12

### Personal – Do's

Individuals are accountable for whatever they put into the public domain even in a privately held account or group. Inappropriate use or inappropriate disclosure of someone else's personal information on social networking and video sharing sites is subject to criminal proceedings (in accordance with section 55 of the Data Protection Act it is a criminal offence to disclose personal information unlawfully) and/or misconduct procedures.

- Use social media channels to communicate essential messaging to the community, e.g.; warn and inform messages from incident or safety advice in line with the prevention strategy.
- Use social media to advertise career opportunities throughout the Service.
- Use social media to promote the Service's values and commitment to diversity and inclusion.
- Be aware that identifying yourself as an employee of SFRS on a personal social media account may expose you to risk. For example, you could become a target, be knowingly primed for information or render yourself, family and friends vulnerable to personal harassment. Therefore, employees are advised to use their discretion in identifying their employment online.
- Show yourself in your best light. If you choose to identify yourself as a SFRS employee within a social network, you are connected to your colleagues and managers. Use a disclaimer. When using social media for personal purposes, you must not imply you are speaking for Shropshire Fire and Rescue Service.
- Avoid use of your or any other fire service personnel's email address, logos or other Service identification.
- Show respect to all. You should be respectful of the Service and your fellow employees. Derogatory comments are always wrong and could potentially expose the author to disciplinary or other legal action.
- Be aware that the media may use social networking sites to gather information about the Service or its staff and are entitled to use anything that is posted.
- Remember that staff in politically restricted roles are prohibited from making any political statements.

### Personal – Don'ts

- Staff who are identifiable as Shropshire Fire and Rescue Service employees i.e. wearing a uniform or using corporate channels, should not post comments which could be judged to express political opinion or be interpreted as attempting to generate public support for any political party or could be interpreted as those of the Service.

- When using social networking sites, blogs and video sharing websites privately, no use may be made of the Shropshire Fire and Rescue Service logo, photographs or images without the express permission of the Service. The corporate communications team can assist. Consideration must also be given to any other matters of copyright.
- Make defamatory comments about Shropshire Fire and Rescue Service, individuals within the Service or partner organisations/ brigade's I.e. making inaccurate comments that would bring the organisation into disrepute whilst easily identifiable as a member of SFRS.
- Staff should not make derogatory comments online whilst being identifiable as a member of SFRS. For example, publishing a review/complaint online whilst having a profile photo in SFRS uniform or having identified yourself as a member of staff on that profile- this is prohibited
- Use social media to bully another individual (such as an employee of the Service or indeed a member of the public)
- Post inappropriate or offensive images, offensive comments, or links to such content – this includes chat platforms such as messenger or WhatsApp amongst others (both members of the public and other members of staff). Employees who engage in abusive or discriminatory conduct towards colleagues or members of the public on WhatsApp could face disciplinary action.
- Reveal any potential confidential or sensitive information about the Service that the employee may be party to as part of their work
- Include contact details or photographs of colleagues, unless consent has first been obtained.
- Use Service email addresses to register on any social media site, unless authorised to do so
- Use social media to liaise with journalists. All requests from journalists for information to be given to journalists will be co-ordinated by the senior officer of corporate communications team.
- Finally, it can be difficult not to comment on a post where the Service is being criticised. Please do not offer your personal views on matters in the public domain or on corporate social media channels. Responses to such issues are agreed at an executive level and posted by the corporate communications team. Feel free to notify the team of any criticisms or defamatory comments you come across on social media.

### **Business – Do's**

- Be aware that identifying yourself as an employee of SFRS on a social media account may expose you to risk depending on your role.
- For example, you could become a target, be knowingly primed for information or render yourself, family and friends vulnerable to personal harassment. Therefore, employees are advised to use their discretion in identifying their employment online.
- Show yourself in your best light. If you chose to identify yourself as a SFRS employee within a social network, you are connected to your colleagues and managers.

- You should ensure that content associated with you is consistent with your work at the Service.
- Avoid use of your or any other fire service personnel's personal email address. Always use a generic mailbox for example recruitment@Shropshirefire.gov.uk ICT can help with details of these mailboxes.
- Show respect to all. You should be respectful of the Service and your fellow employees. Derogatory comments are always wrong and could potentially expose the author to disciplinary or other legal action.
- Individuals are accountable for whatever they put into the public domain even in a privately held account. Inappropriate use or inappropriate disclosure of someone else's personal information on social networking and video sharing sites is subject to criminal proceedings (in accordance with s55 of the Data Protection Act it is a criminal offence to disclose personal information unlawfully) and/or misconduct procedures.
- Staff should be aware that the media may use social networking sites to gather information about the Service or its staff and are entitled to use anything that is posted.
- Remember that staff in politically restricted roles are prohibited from making any political statements.
- Any post relating to the work of SFRS should be factual, already in the public domain and not controversial
- Be prepared for a two-way conversation. And be aware that people are entitled to their views. You must make sure that what you say is factual and avoid unnecessary or unproductive arguments.
- Handle offensive comments swiftly and with sensitivity. If a conversation turns and becomes offensive in terms of language or sentiment, make sure you inform your audience exactly why you have removed the comment. A few sentences should suffice, along the lines of: "This comment was removed because moderators found the content offensive. We will respond to your comments but please respect the views of everybody who comes here."
- Staff who regularly come into contact with young people through youth intervention programmes should make themselves aware of the Child Protection Policy, particularly this paragraph:

Where SFRS employees have worked with or built a professional relationship with young people through the Service's youth intervention programmes they must not under any circumstances, become involved in communications with those young people via social networking sites or other electronic communication methods such as text messaging.

In such circumstances an approach from a young person (under the age of 18) should be rejected and deleted where necessary.

Breach of this obligation is likely to be viewed as gross misconduct.

## **Business – On Service accounts you should not:**

- Criticise or argue with the public, colleagues, or any other affiliates of the Service – this includes communications on all social media channels including Whatsapp
- Make defamatory comments about Shropshire Fire and Rescue Service, individuals within the Service or partner organisations/ brigade's I.e. making inaccurate comments that would bring the organisation into disrepute whilst easily identifiable as a member of SFRS
- Use social media to bully another individual (such as an employee of the Service)  
Post inappropriate or offensive images, offensive comments, or links to such content – this includes chat platforms such as messenger or WhatsApp amongst others. Employees who engage in abusive or discriminatory conduct towards colleagues or members of the public on WhatsApp or any other social media platform could face disciplinary action.
- Comment on sensitive business-related topics or financial information
- Divulge confidential information about the Service itself, its customers, or suppliers
- Unless authorised to do so, do not post pictures of yourself wearing uniform. Be aware that by identifying yourself as an employee of SFRS on a personal social media account may expose you to risk. For example, you could become a target, be knowingly primed for information or render yourself, family and friends vulnerable to personal harassment. Therefore, employees are advised to use their discretion in identifying their employment online.
- Reveal any potential confidential or sensitive information about the Service that the employee may be party to as part of their work
- Include contact details or photographs (without written consent to do so) of colleagues and who to contact if removal of content is required in the future i.e. the Communications Team
- Reveal any potential confidential or sensitive information about the Service that the employee may be party to as part of their work
- Include contact details of colleagues or photographs unless you have written consent.
- Disclose any information in breach of General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Use Service email addresses to register on any social media site, unless authorised to do so
- Use social media to liaise with journalists. All requests from journalists for information to be given to journalists will be co-ordinated by the senior officer of corporate communications team