Essex County
Fire & Rescue Service

SOCIAL MEDIA POLICY

About

This policy explains the appropriate use of social media channels both inside and outside the workplace.

This Policy should be read in conjunction with Employee Code of Conduct and ICT Acceptable Use Policy.

Index Page

1 POLICY STATEMENT

1.1 Essex Police, Fire and Crime Commissioner Fire and Rescue Authority ("the Service") uses a range of techniques to communicate internally and externally in order to fulfil the Service's objectives efficiently, effectively and in line with the law. The Service welcomes innovation in communications and will continue to develop the use of social media to increase the impact of messages.

1.2 The Service supports freedom of expression and this policy sets out standards for employees to be able to exercise this right appropriately, safely, legally and in line with Service policies.

1.3 Any communication that employees make in a professional capacity are subject to the rules below. Communications in a private capacity which have the scope to affect the Service or its employees are also subject to these rules. The following are potential examples of unacceptable use (this is not intended to be an exhaustive list):

- Revealing any potentially confidential or sensitive information about the Service that the employee may be party to as part of their work.
- Using any FRS logos, images or copy-righted material.
- Including contact details or photographs of colleagues.
- Including photographs of incidents or work locations.
- Making offensive comments about colleagues, the Service or members of the public.
- Disclosing any information in breach of the Data Protection Act.
- Using social media as a means of bullying and intimidation.

1.4 This policy statement is supported by the Article 10, Freedom of expression and Article 11, Freedom of assembly and association, of the 'Human Rights Act 1998'. Everyone has the right to freedom of expression and the privacy of this workforce to a family and private life in home and correspondence. People at work have the right to express their views without running the risk of being disciplined, dismissed or victimised. However, a distinction must be drawn between expressing an opinion and disrupting the workplace or creating an unhealthy atmosphere by making offensive, slanderous or damaging remarks or gestures to colleagues, clients, customers or members of the public and to create a workplace free from unlawful discrimination, harassment or bullying. This extends to social media.

2 SCOPE

2.1 This policy applies to all employees of the Essex Police, Fire and Crime Commissioner Fire and Rescue Authority (the Authority). This includes temporary staff, agency workers, volunteers, those on secondments and third party associations affiliated to the Service.

2.2 The policy covers:

a) communication in the performance of an employee's duties

b) communication in a wider context where there is an impact on other employees or the Service.

3 DEFINITION

3.1 Social media are interactive online platforms that allow parties to communicate instantly with each other or to share data in a public forum.

3.2 This includes online social forums such as Workplace, Twitter, Facebook, LinkedIn and Pinterest and messaging services such as WhatsApp and Snapchat.

3.3 Social Media also cover blogs and video and image-sharing websites such as Instagram, Snapchat, TikTok and YouTube.

3.4 There are many more examples of social media and as such the above examples are not an exhaustive list.

3.5 Employees should follow this policy in relation to any and all social media that they use.

4 PROFESSIONAL USE

4.1 Employees are encouraged to utilise relevant professional platforms in the course of their work. The benefits include positive communication, professional networking, developing knowledge and expertise and educating employees or the public. This includes maximising the potential of the NFCC's Group on Workplace, as well as other FRS related groups on this channel.

4.2 Contributions can be made to the Service's official blogs, Twitter page and Facebook pages. Guidance should be obtained from the "house rules" on the ECFRS corporate Facebook page.

4.3 Employees must be aware at all times that while contributing to Service social media activities they are representing the Service.

4.4 Employees who use social media as part of their job must adhere to the following rules:-

a) use the same safeguards as they would with any other form of communication about the organisation in the public sphere;

b) ensure the communication has a purpose and a benefit for the Service;

c) have obtained permission from the Corporate Communications Team before embarking on a public campaign using social media;

d) ensure a manager has checked the content before it is published.

4.5 It is accepted that people use social media to exchange informal work related information, such as WhatsApp, Skype/ Lync. This may be permitted where stringent standards are followed as in paragraph 1.3. Furthermore, it must not be used where confidentiality would be breached. Employees using these mediums should ensure that no one is deliberately ostracised and do their utmost to ensure no one is unintentionally excluded based on them not being a member of the group. Caution should be taken regarding the use of humour or any other comments which might be misunderstood and so cause distress. Should any adverse impact be noted from any social group employees are advised to stop using them until good practice can be ensured.

5 PERSONAL USE AT WORK

5.1 Employees are allowed to access Social Media websites from work computers or devices for their personal use during official rest breaks.

5.2 There are sites which are specifically blocked or have restricted access. Employees should understand that this is to protect the Service's information systems from malware and also to avoid access to unsuitable content.

5.3 Employees may wish to use their own computer or devices such as laptops to access social media websites while at work. Again, this will be permitted during official rest breaks. Employees should not spend an excessive amount of time while at work using social media websites.

6 PERSONAL USE OUTSIDE OF WORK

6.1 The Service recognises that many employees make use of social media in a personal capacity. While they are not acting on behalf of the Service, employees must be aware that they can damage the Service if they are recognised as being one of its employees. Employees must not use the Authority's logos or other copyright material on any personal social networking communications or in the information contained within your profile.

6.2 Employees are allowed to say that they work for the Service, which recognises that it is natural for its staff to want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) must not contain the Service's name.

6.3 The Service will investigate any online / social media activity by employees which raises safeguarding concerns for individuals, organisations, and their family of community.

7 STANDARDS GOVERNING ALL ONLINE ACTIVITY (AT WORK AND OUTSIDE OF WORK)

7.1 All postings, either personal or professional, which suggest a link to the Service must be done in line with legal requirements, in particular the Equalities Act 2010 and the Data Protection Act 2018, and in accordance with Service Values.

7.2 Any posts relating to the work of the Service should be factual, already in the public domain and not controversial.

7.3 Employees should exercise caution and be careful to avoid, either consciously or inadvertently, 'liking', 'favouring' or 'forwarding the content of' any sites that could be perceived to be posting inappropriate comments or content. Inappropriate comments and content include but are not limited to discriminatory, offensive material and pornography.

7.4 Everyone has the right to freedom of expression. People at work have the right to express their views without running the risk of being disciplined, dismissed or victimised. However, a distinction must be drawn between expressing an opinion and making offensive, discriminatory, slanderous or damaging remarks or gestures to co-workers, clients, customers or members of the public.

7.5 Employees and the Service must give acknowledgement where permission has been given to reproduce or use someone else's images or written content. You must gain written consent before taking any pictures or making any recordings on behalf of the Authority for social media or general communications use. Employees must not use the Authority's logos or other copyright material on any personal social networking communications or in the information contained within your profile.

7.6 The Service uniform represents the image of the organisation and employees should therefore ensure that, if they are photographed wearing the uniform, it is in a manner that is appropriate and respectful.

7.7 Employees must not photograph or film an operational incident unless they have specific work requirements to do this.

7.8 Employees must not respond to the Press and Media on behalf of the Authority through any social media platforms unless they have engaged with the Corporate Communications team.

7.9 Employees must not use open social media channels to raise or discuss any work related grievances. All employees should pursue work related grievances via the agreed grievance policy.

7.10 Employees should not do anything that could be considered discriminatory or to constitute bullying or harassment, including trolling, of any individual or group, for example making offensive or derogatory comments relation to race, ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health data, sex life, or sexual orientation. ACAS guidance defines cyber bullying as *'bullying, harassment and victimisation conducted through social media such as blogs or social networking sites. Inappropriate photographs; offensive or threatening comments; or sensitive personal information could be revealed. This could be done accidentally or vindictively.'*

7.11 There is a risk to both uniformed and support staff from the misuse of any social media sites. Inappropriate content or posts may give grounds for complaint to and or disciplinary action by the service. If in any doubt, contact the HR team who will be able to give appropriate guidance.

7.12 Employees should not write a blog in an official capacity, i.e. representing the views of the Service without expressed permission of the Corporate Communications team. If, however, employees choose to give a personal opinion as an experienced person in a particular field, they are required to state that it is solely their views and not the view of the Service.

7.13 Employees must not use any Service logos or other copyright material on any of their personal social networking communications or in the information contained within their profile details, to avoid giving the inference of official service endorsements. Communications in this instance shall include all photos, articles, documents or opinions.

7.14 In order to prevent any photos/footage being uploaded to social media sites that may compromise the Service, e.g. inadvertently posting photos of an incident that is a crime scene or that may be insensitive to victims, e.g. photos/footage of a house fire that enables identification of an individual property or person, photographs or footage of any operational incident must only be taken by either the Officer in Charge of the incident who will liaise with the Corporate Communications team over appropriate use.

7.15 The Service fully recognises the role of trade unions within the workplace and respects their rights and need to function in line with their own objectives. The Service also recognises that there will be times when these objectives will differ to that of the Service and the officials/members within that trade union will campaign against a decision made by the Service on political or strategic matters and some of this campaigning will take place via social media. In such circumstances both trade union representatives and ECFRS managers should be mindful of the NJC circular on 'joint protocol for good industrial relations' and its commitment to working together for the benefit of the Service and a 'no surprises culture'. This extends to the use of social media.

8 MONITORING USE OF SOCIAL MEDIA AT WORK

8.1 The Service reserves the right to monitor employees' internet usage whilst using Service equipment, and will inform them when this is to happen and the reasons why.

8.2 The Service believe that valid reasons for checking employee's internet usage include suspicions that the employee has:

- Been using social media websites excessively when they should be working (monitoring will only be carried out as part of a performance improvement plan)
- Acted in a way that is in breach of the rules set out in this policy.
- Acted in a way that is in breach of the rules set out in Employee Code of Conduct (section - Use of Email and The Internet)
- Potentially caused a data breach as defined in the Data Protection Policy.

8.3 The Service reserves the right to retain information gathered on employees' use of the internet for a maximum period of one year.

8.4 Access to particular social media websites me be restricted or withdrawn in any case of misuse.

9 USE OF SOCIAL MEDIA IN A RECRUITMENT PROCESS

9.1 Unless it is in relation to finding candidates (for example, if an individual has put their details on social media websites for the purpose of attracting prospective employers – for example, LinkedIn), the HR department and managers will not, either themselves or through a third party, conduct searches on applicants on social media.

9.2 There should be no systematic or routine checking of prospective employees' online social media activities, as conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the Service's Equality and Diversity policy.

10 MISUSE OF SOCIAL MEDIA

10.1 Employees are required to adhere to this policy.

10.2 Employees should note that any breaches of this policy may lead to disciplinary action.

10.3 Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the Service, may constitute gross misconduct.

10.4 Employees who are on sick leave should consider the appropriateness of using social media sites to place posts which may be deemed to be in conflict with any aspects of the current Attendance Management Policy.

10.5 See Toolkit - Assessment Matrix.

11 LINKS TO OTHER POLICIES AND PROCEDURES

- Code of Conduct
- Data Protection Policy
- Equality and Diversity Policy
- Dignity at Work Policy
- ICT Acceptable Use Policies

- Disciplinary Policy
- Grievance Policy
- The Prevent Agenda

Frequently Asked Questions relating to this policy are available on the intranet.

If you would like to speak to someone about this policy please call the HR Support Team on 01376 576199 or email HR-Support.