

Police, Fire and Crime Commissioner for Essex

Social Networking Policy

Version Control	Version 1.4	April 2020
Reviewed By	D Horsman	November 2019
Policy owner	P Brent-Isherwood	April 2020
First Published	J Drewett	January 2013
Next Review Date	D Horsman	April 2023

Version history

Version Number	Date	Reason for review	Comments
1.0	January 2013		First publication
1.1	February 2016	Policy update	Minor amendments
1.2	September 2017	Scheduled review	Minor amendments
1.3	November 2019	Scheduled review	Minor amendments
1.4	April 2020	Review by Monitoring Officer	Updated to cover social media usage both in an official capacity and outside of work. Section 2 updated.

1.0 About this Policy

This policy outlines the responsibilities of all staff, whether permanent or temporary, when using the internet together with social networking forums, whether in an official capacity or when publishing online content whilst outside working hours. It provides a structured approach to social networking and aims to ensure that:

- A consistent and corporate approach is adopted and maintained relating to the use of social media;
- Information held by the PFCC and their staff remains secure and is not compromised through the use of social media;
- The use of social media is effective, lawful and does not compromise the computer systems or networks owned or maintained by the PFCC or Essex Police, and
- The PFCC's reputation is not damaged or otherwise adversely affected by the use of social media.

A social networking site, for the purpose of this policy, is defined as a category of media where people are talking, participating, sharing, networking and bookmarking online. Whilst not an exhaustive list, prominent examples would include Facebook, Twitter, Instagram, Snap Chat, You Tube, Flickr, Pinterest, LinkedIn and group messaging services such as WhatsApp.

2.0 Risk Assessments / Health and Safety Considerations

The following risks have been identified with social media usage, though it should be noted that this list is not exhaustive:

- Failure to comply with this policy may compromise the security of the Police, Fire and Crime Commissioner (PFCC) for Essex; their staff and the information that they hold. The internet, including social media accounts, may be used by criminals to target the PFCC and their staff. Personal details can often be used to manipulate a member of staff to reveal sensitive or confidential information. Computer systems and networks may be infected with viruses or other malware (malicious software) transmitted via social media.
- Failure to comply with this policy may compromise the reputation of the Police, Fire and Crime Commissioner (PFCC) for Essex.
- Civil or criminal action relating to breaches of legislation.
- Social engineering attacks (also known as "phishing").
- Safeguarding risks brought about through the use of images leading to the abuse or exploitation of vulnerable children or adults.

If any member of staff receives any threat, abuse or harassment from a member of the public or another organisation through their use of social media as part of their work, they must report this immediately to their line manager.

3.0 Policy

Social Networking in a Private Capacity

The PFCC recognises an individual's right to a private life outside of work and understands that social networking sites are a way for people to maintain contact with friends and family. However the PFCC also has a duty to ensure that inappropriate use of information through these sites does not jeopardise:

- The safety of staff;
- The organisation's reputation or public confidence in it, or
- The confidentiality of any information assets retained by the organisation.

Members of staff are legally responsible for anything they write or do online. Anything they say or do could be interpreted as representing the views of the PFCC where they could be identified as being a member of the PFCC's staff. The law of defamation applies to social media in the same way as to other written or spoken communications. As such, the PFCC and / or an individual member of staff can be sued for damages if a person or business considers that their reputation has been or may be damaged as a result of their actions on social media. Staff should take care not to make any libellous statements (that is, statements that lower the reputation of a person or organisation) on social media or any other online platforms.

All staff are required to ensure that, when using social networking sites and other online media in a private capacity, they do not:

- Conduct themselves in a way that is detrimental to the PFCC. This includes maliciously undermining the PFCC's decisions or staff through adverse or negative comments;
- Bring the PFCC into disrepute by expressing extreme views;
- Participate in any interaction which could damage working relationships between staff, partner agencies, members of the public, or other stakeholders;
- Make defamatory or offensive comments about the service provided by the PFCC including Essex Police, the Essex County Fire and Rescue Service, partner agencies, or other stakeholders;
- Make remarks about any individual, including other PFCC staff or members of the public, which may be considered offensive or discriminatory, or which otherwise do not comply with the Equality Act 2010 and associated legislation;
- Share any personal issues concerning their employment;
- Share confidential information about the PFCC, its officers, staff, services, partner agencies, members of the public, or other stakeholders;
- Discuss private information about others that they have learned through their work;
- Post or publish any written or pictorial material obtained or gathered during the course of their work;
- Display any photograph or image of themselves in circumstances likely to undermine the reputation of the PFCC;
- Use a work-related email address when registering with social media sites for personal use,

- Mislead readers into believing that any material published by them is posted on behalf of, or authorised by, the PFCC if it is not; or
- Join or show support (e.g. by “liking”) any group or organisation likely to undermine the integrity or impartiality of the staff member.

In order to avoid breaches of the above, staff are advised to refrain from discussing anything that relates to the PFCC or their employment other than in general terms, i.e. ‘had a good day at work’. Staff must not use personal social media accounts to publish or report on meetings or agenda items which are restricted or internal.

All PFCC staff, other than the Deputy PFCC, are also reminded that they are politically restricted and should have due regard to this in their use of social media. Any sharing of information could be seen as an endorsement of a particular view, individual or organisation, and it is important that the PFCC’s staff remain impartial. This applies at all times but is especially important in any pre-election or “Purdah” period.

Staff members must be aware that social networking websites are often a public forum and should not assume that their entries on any website will remain private. Staff should also be mindful that, once published online, content is almost impossible to control and may be manipulated without their consent, used in different contexts or further distributed. Even closed discussion groups as those found on Whats App can often find their way into the public domain and may result in a breach of this policy. These forums may be used by criminals to target staff members seeking to gain their trust in order to infiltrate the organisation or those associated with it.

Staff must therefore take responsibility for their online security and take steps to protect themselves from identity theft by restricting the amount of personal information they provide. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team. Such details are often used to form the basis of security questions and passwords. Staff are advised to check their online privacy settings so that they can properly understand who can view their personal information and see the information they publish, and must ensure that no information is made available that could provide a person with unauthorised access to PFCC or Essex Police systems.

Social Networking on behalf of the PFCC

The PFCC’s office has its own official Facebook and Twitter accounts, which are generally monitored during office hours only. The use of social media increases the accessibility of our communications to local residents and businesses. It enables the PFCC and their staff to be more active in their relationships with residents, partners and stakeholders and encourages people to be more involved in local decision-making, ultimately helping to improve the services that we provide.

Any member of staff wishing to tweet or otherwise post on social media on behalf of the PFCC’s office should gain approval from either the Strategic Head of Policy and Public Engagement or the Communications and Engagement Manager. Staff are not to set up any social media accounts, groups, pages or profiles, or take part in any social media activity on behalf of the PFCC without first gaining such approval. As part of this process, a moderator must be agreed for each authorised account, group, page or profile.

Training has been provided on how to effectively use social media and ongoing guidance is available from either the Strategic Head of Policy and Public Engagement or the Communications and Engagement Manager. Advice should be sought prior to posting content if the members of staff is unsure of what to.

Staff who publish content on social media sites in the course of their employment are personally responsible for any such content. When social networking on behalf of the PFCC's office, as well as complying with the guidelines applying to social media usage in a private capacity (set out above), staff should:

- Engage actively with local residents, businesses and visitors, answering their questions and responding to their comments quickly and honestly;
- Share other organisations' helpful content and links;
- Use hashtags appropriately to publicise calls to action or events, and
- Ensure they have permission to use any photographs or videos of people before publishing them.

When social networking in an official capacity, staff may follow or "like" people or organisations that provide information that is pertinent to the work of the PFCC or those whose information can usefully be passed on for the benefit of Essex residents, businesses and visitors. However the PFCC's official social media accounts must not be used for party political purposes or specific party political campaigning purposes. The incumbent PFCC may, however, use their own personal social media accounts for these purposes.

We reserve the right to remove from our social media accounts any contributions that contravene the rules and guidelines of the relevant site, use foul or abusive language, and / or which are considered to be:

- Distasteful or irrelevant;
- Unlawful, libellous, harassing, defamatory, threatening, harmful, obscene, profane, sexually orientated, sexist or racially offensive;
- A breach of copyright;
- Revealing of any individual's personal information;
- Advertising products or services, or
- Political in nature.

Copyright laws apply online as they do in any other environment. Posting images or text from a copyrighted source (e.g. photographs or extracts from publications) without permission is likely to breach copyright. If staff are unsure about publishing copyrighted material they must seek permission from the copyright holder in advance.

4.0 Monitoring and Review

It is every manager's responsibility to ensure that this policy is adhered to by their staff. As such, they may review and investigate the use of social media by their staff whenever a complaint or concern is raised.

Any staff member who breaches this policy may be liable to criminal or disciplinary action in accordance with the Code of Conduct and Staff Discipline Procedure. Other violations arising from the contravention of this policy, such as breaches of the Data

Protection Act, could lead to fines being levied against the PFCC and potentially civil or criminal action being taken against the PFCC and / or the individual(s) involved.

This policy will be reviewed by or on behalf of Police, Fire and Crime Commissioner within three years of the date of publication to ensure that it remains fit for purpose. Such review may take place earlier if required by changes in legislation, regulations or best practice.

5.0 Related Policies and Procedures

- Use of Communications Policy
- Staff Code of Conduct
- Staff Discipline Procedure
- Confidentiality Declaration
- Data Protection Policy
- Ethics and Integrity Framework

6.0 Information Sources

- Related Essex Police policies and procedures