

PROCEDURE – Private and Professional Use of Social Media Websites

Number: C 3011

Date Published: 25 May 2018

1.0 Summary of Changes

This procedure has been updated to include the online use of social media for both private use and accounts held as Essex Police employees; the title has been changed to reflect this. The owner and author details have also been updated.

2.0 What this Procedure is about

This procedure provides guidance and outlines the responsibilities for Essex Police employees and all members of the police 'family' including contracted staff, volunteers and agency workers when using social media. Throughout this procedure 'employees' will be referred to, which is to include police officers, contracted staff, volunteers and agency workers for the purpose of this procedure.

Social media should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chatrooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others.

Reference is made to both personal and professional accounts held by employees for use both on, and off duty.

Essex Police recognises an individual's right to a private life and understands that online forums and social networking sites are a way for people to maintain contact with friends and family, having a reasonable expectation of privacy when it comes to separating private lives from the workplace.

This document has therefore been drafted to comply with the principles of the Human Rights Act and a proportionate approach has been taken to ensure compliance; whilst protecting Essex Police as an organisation and those who work within.

Employees should all have an awareness and understanding of the Code of Ethics, as such we must all comply to those standards of behaviour whether on or off duty, and whether on or off line.

Officers and staff are also reminded of their obligation to comply with 'Police Regulations' and 'Police Staff Standards of Professional Behaviour'.

This procedure should be read in conjunction with the following:

- Stay safe online guidance
- Training Twitter 2016

Compliance with this policy and any linked procedures is mandatory.

PROCEDURE – Private and Professional Use of Social Media Websites

Number: C 3011

Date Published: 25 May 2018

3.0 Detail the Procedure

As a general rule, any information which would fit into one of the below 3 categories should not be written or shared;

- If it breaches information security rules;
- If it poses a reputational risk to Essex Police;
- If it puts the safety of Essex Police employees or volunteers at risk.

If any content breaches these criteria, then the individual could be subject to a misconduct process or criminal proceedings.

3.1 Information Security

Employees are not to publish post or release any information that would be considered private or confidential or protectively marked..

Employees must not reveal operational material or tactics that are not in the public domain.

3.2 Reputational Risk

Employees are responsible for anything they write or share online. The simple rule to remember is that the principles covering the use of social and other digital media in both a work and personal capacity are the same as those that apply for any other activity.

Employees need to know and adhere to the standards set out within the Code of Ethics when using social media and online forums. Social media is a public forum and the same considerations would apply as speaking in public or writing for a publication.

In social media the boundaries between professional and personal are often more blurred – so it's important to be particularly careful.

There can be no expectation of privacy regarding anything posted online regardless of the account holders' privacy settings. There is no guarantee of others' privacy settings or intentions. Access to the information written or shared could be circulated wider or accessible to all online. Information placed on the Internet or social media could potentially end up accessible worldwide. When you are posting on the internet, your integrity is on display for all to see. Therefore, any information placed on the Internet / social media could become a public disclosure.

Employees must also remain mindful when sharing information in private or closed group forums. Whilst there is an expectation that sharing information in private should remain so, control of any media once shared with others can be at risk of being shared wider and made public online. Employees should therefore remain mindful of

PROCEDURE – Private and Professional Use of Social Media Websites

Number: C 3011

Date Published: 25 May 2018

the viral effect of the internet and social media. The potential for the smallest piece of information can be scaled up beyond all expectations.

3.3 Officer and Staff Safety

If employees encounter a situation whilst using social media that could cause a risk to any person or to the organisation, this should be brought to the attention of the line manager immediately so a risk assessment can be made and appropriate action / safeguarding undertaken.

3.4 Personal Social Media Account

Officers and staff should consider the implications of discussing or posting anything that relates to the organisation or their employment.

Use of a personal social media account must still be done in line with Code of Ethics, with potential implications for the officer or staff member if they breach the police officer code of conduct or police staff standards of professional behaviour.

Posting any image or information that links them to the Police Service could identify them and put them at risk so should be assessed carefully before placing this on any social media. Online forums can be used by criminals to target police officers or members of staff, seeking to gain their trust in order to infiltrate the organisation. This is also a step to ensure personal safety. Employee's safety is a priority for Essex Police and any unsafe online use can expose their affiliation to the organisation which could be considered a target from certain crime groups.

Criminals and others may seek to use the Internet and social media to identify personal information about Essex Police employees with a view to embarrassing, discrediting, harassing, corrupting or blackmailing them or their families for their own benefit.

Employees must therefore take responsibility for their online security and take steps to protect themselves by restricting the amount of personal information they provide. Details recorded online such as date of birth, place of birth and favourite football team are often used to form the basis of security questions and passwords.

PROCEDURE – Private and Professional Use of Social Media Websites

Number: C 3011

Date Published: 25 May 2018

3.5 Professional Social Media Account

The rapid growth in the public use of social networking has provided significant new opportunities to make contact and consult with communities. Professional Essex Police twitter accounts can be created in consultation with the media department for your use, so information can be shared and written relating to work matters which promote positive messages about Essex Police and the work the organisation is undertaking.

Employees are encouraged to embrace the many benefits available through effective use of the Internet and social media. Such benefits can include more effective communication with communities, more informed consultation and local engagement, and an opportunity to demonstrate greater accountability and transparency.

Employees who use professional social media accounts may generate media enquiries from the details they post. Employees should feel confident to manage those media enquiries but seek help and guidance from the press office where needed.

Essex Police computers may be used for professional social media account use and for work purposes. Personal accounts must not be accessed through Essex Police computers.

Social media use to research individuals or detail about an incident or investigation needs to adhere to the correct process and authorities.

Alongside all the benefits that this brings we need to be aware of the responsibilities that come with it, and ensure we maintain the highest level of propriety.

4.0 Equality Impact Assessment

Equality and Diversity issues have also been considered to ensure compliance with the Equality Act 2010. In addition, Data Protection, Freedom of Information and Health and Safety Issues have been considered. Adherence to this policy or procedure will therefore ensure compliance with all relevant legislation and internal policies.

5.0 Risk Assessment

Failure to comply with this procedure may compromise the reputation and security of Essex Police.

Failure to comply with this procedure may compromise the safety and security of Essex Police employees and the estate.

PROCEDURE – Private and Professional Use of Social Media Websites

Number: C 3011

Date Published: 25 May 2018

The internet can be used by criminals to target officers and staff. Personal details found online can be used to identify the details of home addresses and family of employees; they can also be used to manipulate an officer or member of staff to reveal sensitive or confidential information.

Decision making will follow guidance as provided by the National Decision Making Model (NDM) and due regard will be given to the principles and standards contained in the Policing - Code of Ethics.

6.0 Consultation

The following were invited to provide feedback in the consultation phase during the formulation of this document:

- Unison
- Police Federation
- Essex Diversity and Inclusion Manager
- Health & Safety
- Strategic Change Team
- PSD Superintendent
- Policy/Risk
- Superintendents Association
- Media Department
- HR
- IT
- Information Management
- SCD

7.0 Monitoring and Review

This procedure will be monitored by or on behalf of the Head of Professional Standards every 12 months, given the fast moving online and social media progress to ensure that it remains fit for purpose.

8.0 Governing Force policy. Related Force policies or related procedures

- C 3000 Policy - Professional Standards
- W 1001 Procedure/SOP – ICT Acceptable Use
- W 1004 Procedure – Incident Reporting and Management
- L 1200 Protocol - Police Staff Discipline
- A 08 Strategy - Digital Policing

PROCEDURE – Private and Professional Use of Social Media Websites

Number: C 3011

Date Published: 25 May 2018

- A 0600 Policy - Community Policing
- S 2000 Policy - Covert Policing
- S 2800 Policy - Open Source and Social Media
- S 2801 Procedure - Open Source and Social Media
- W 1000 Policy - Information Management and Assurance

9.0 Other source documents, e.g. legislation, Authorised Professional Practice (APP), Force forms, partnership agreements (if applicable)

- Police Conduct Regulations 2012
- College Of Policing APP Engagement and communication
- Data Protection Act 2018
- General Data Protection Regulations (GDPR)
- The European Convention on Human Rights (ECHR) 1998
- The Code of Ethics
- Guidance – Stay Safe Online

Cancellations: None