USE OF PERSONAL DEVICES AND THE MANAGEMENT OF RISK ASSOCIATED WITH THEIR USE

Owning Department: Professional Standards/Information Management

Department SPOC: D/Sgt Service Improvement Unit (PSD) / Information Security Manager

Governing Policy: Uniform, Appearance and Standards

Risk Rating: Medium Low

Legal Sign Off: 17/12/2020

JNCC: December 2019

Published Date: 02/02/2023 (v1.1)

Review Date: 01/02/2026

Index

1. Summary of Changes

1.1 This procedure has been updated to complement the Acceptable Use of Information Systems and Assets policy and procedures and should be read in conjunction with those documents.

2. Procedure Aim

2.1 This procedure provides guidance on the use of personal devices and personal online accounts (e.g. social media) whilst on and off duty.

2.2 The use of the internet and social media by police officers and staff carries with it an element of risk that those working for Norfolk or Suffolk Constabulary need to be aware of. This document outlines the action that officers and staff should take to mitigate those risks.

2.3 These risks include:

- Breach of trust and confidence – Disclosure of information obtained by the police service or partners, about the police service, partners or colleagues.
- Unauthorised disclosure of personal data – breach of the Data Protection Act 2018 and the General Data Protection Regulations.
- Bringing discredit on the police service or its partners.
- Revealing personal information about yourself or your family – increased vulnerability to harassment, corruption or blackmail.
- Revealing operational material or tactics.

3. Guiding Principles

3.1 The public expect police officers and staff to process their personal data carefully and sensitively. The Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR) places obligations on Controllers to ensure that personal data is processed in accordance with the data protection principles. Failure to do so could lead to serious

consequences for the Constabularies. Therefore, every officer and member of staff has the responsibility to keep personal data they are processing secure and compliant with the Data Protection legislation (DPA and GDPR). More information regarding our obligations can be found in the Data Protection Policy.

3.2 Public confidence in the police service depends on all officers and staff demonstrating the highest level of personal and professional standards. The Code of Ethics sets out the ethical principles which guide the actions of officers and staff. These principles apply to on line behaviour in the same way as they do to off line activity, especially where it can undermine public confidence in the Constabularies.

3.3 Officers and staff have a right to a private life and this includes their on-line activity. It is still possible, however, for private on-line activity to breach the Standards of Professional Behaviour and the Code of Ethics, especially where their off duty on-line conduct can be linked to the Constabularies.

4. Applicability

4.1 Unless otherwise stated the guidance applies to all police officers and police staff.

4.2 This document should not be interpreted as an exhaustive list of rules, but highlights the risks and action that officers and staff can take to prevent a Breach of the Code of Ethics or the Standards of Professional Behaviour or expose the organisation or them to harm.

5. Digital Footprint

5.1 A digital footprint is the data that is left behind whenever a digital service is used, or whenever someone posts information about somebody onto a digital forum, such as a social network.

5.2 Having a digital footprint is normal; they are very difficult to avoid. Given that a digital footprint is publicly accessible, it is recommended that everyone should know exactly what theirs looks like and how to actively manage it.

6. Use of Constabulary Owned Assets

6.1 Norfolk and Suffolk Constabularies provide access to various information assets for use in the course of and/or in connection with police business. Personnel with authorised access have responsibility for all data processing that is performed by them and must adhere to the relevant laws including; General Data Protection Regulation (GDPR) and Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1998 as well as force policies and procedures. Failure to comply with legislation, force policy and procedure may result in disciplinary and potentially, criminal or civil proceedings.

6.2 The Telecommunications (Lawful Business Monitoring) (Interception of Communications) Regulations 2000 allows for the monitoring of the activities of personnel using Constabulary owned assets. This monitoring includes all personal, as well as business communications, and applies to all police ICT devices including mobile devices. Where there is believed to have been a breach in the security of police information this must be reported to Information Security or the Professional Standards Department. The Lawful Business Monitoring policy should be referred to.

6.3 Everything that is owned by the Constabularies which officers and staff use for their role and to carry out the business of Norfolk and Suffolk Constabularies is classed as an asset owned by the Constabularies. This includes the following (not an exhaustive list):

- Computers,
- Laptops,
- Police Radios,
- Mobile Data Devices,
- Mobile Phones etc.

6.4 The Constabularies do not allow use of force assets for personal use.

7. Use of Personal Devices

7.1 The use of personal devices for any Policing purpose is **NOT** permitted.

7.2 Officers and Staff should be aware that work related images or data, taken or stored on personal devices are not secure and sit outside of the protected network provided by the organisation. They are therefore more vulnerable to loss. Police information stored on a personal device may represent a data breach and therefore personal devices should not be used to communicate police information, including images.

7.3 Use of personal devices during work time should be avoided as much as possible, however incidental use is permitted where practical, e.g. sending a quick text message, answering a call. Users should be mindful of their usage whilst at work and keep it to a minimum and not use their personal device in public view.

7.4 Due to the potential risks to the security of the user's personal information and that of their family and their friends, all officers and staff should be aware of the need to protect themselves and their personal information online, especially whilst using social media accounts. Officers and staff can take steps to protect their personal information by following the latest guidance.

7.5 All officers and staff are accountable for any information placed in the public domain, even if it is a privately held account. Officers and staff should be aware of the potential for their on-line conduct to discredit the

Constabularies, undermine public confidence in the service and/or breach the Code of Ethics or the Standards of Professional Behaviour.

7.6 Personal social media accounts must never be used for Constabulary purposes in any circumstances, as per the Internet Intelligence and Investigations policy.

7.7 When posting information on social media sites, both personal and corporate, consider the risks of the following:

- Your personal safety and exploitation of your personal information – avoid providing addresses, phone numbers, email addresses etc.
- The security of information relating to family, friends and other contacts.
- The welfare, safety and privacy of colleagues, customers/next of kin.
- The security of the organisation.
- The integrity of operations and investigations.
- Any direct reference to the user's role or the organisation on personal accounts.

7.8 Officers and Staff should be careful to not link any political opinions to their occupation to ensure that the organisation continues to demonstrate a transparent and unbiased position. This also applies to personal social media accounts and postings which could inadvertently link the person's relationship with the Constabularies to their own political opinions.

7.9 Please refer to the Social Media Guiding Principles document for further advice and guidance.

8. Security

Operational Security

- Officers and Staff should be aware of the potential significant security implications of using any form of social media or the posting of photographs during worktime or within/ on police premises. Many applications contain metadata which links the user to locations, which could increase the risk to operational security if covert locations or vehicles etc are then identified. When using a mobile device consider turning off any GPS/location tracking options within social media apps that identify the user's location.

- Officers and Staff could also inadvertently disclose sensitive police information within the background of photographs taken. Any images of this kind can represent a data breach and should be reported accordingly.

Personal Security (and that of the Officer's/Staff member's family etc.)

- All officers and staff need to maintain responsibility for their own personal safety and that of their family and colleagues. This responsibility extends

beyond traditional physical measures and needs to encompass an individual's digital presence to prevent access to personal information which could be used to identify and locate them.

- Police Officers and Staff hold a unique position within society, which affords them access to highly sensitive and confidential information. Such access could leave them vulnerable to the risk of coercion, blackmail or corruption from those who would seek to use this information to their advantage.

- The risk to Police from terrorism is a constant threat and it is vital that officers and staff maintain responsibility for their personal safety by regularly checking the privacy and location settings on their personal devices and linked social media accounts to prevent individuals being identified as Officers or Staff.

Geo Location

- Officers, while on duty, are advised to switch off geo location on personal devices to mitigate any risks of identifying themselves at locations that could pose a risk. Unintentionally officers and staff are continuously advertising where they are and locations they are at through various apps such as Strava/Facebook/Instagram.

- This functionality poses huge risk to individuals and the organisation against those groups or people who have a dislike for the police and their officers and staff.