LAWFUL BUSINESS MONITORING

Owning Department: Professional Standards
Department SPOC: Det Insp, ACU
Risk Rating: Low
Legal Sign Off: 09/12/2022
JNCC: Sept 2022
Published Date: 13/12/2022 (v1)
Review Date: 12/12/2026

Index

Legal Basis

Legislation specific to the subject of this policy document:

- Investigatory Powers Act 2016
- Computer Misuse Act 1990
- Investigatory Powers (Interception by businesses etc. for Monitoring and Record Keeping Purposes) Regulations 2018
- Human Rights Act 1998
- General Data Protection Regulation (2016/679)
- Data Protection Act 2018
- Regulation of Investigatory Powers Act 2000

Other relevant legislation which you must check this document against (required by law)

- Equality Act 2010
- Crime and Disorder Act 1998
- Health and Safety at Work etc. Act 1974 and associated Regulations
- Freedom Of Information Act 2000
- The Civil Contingencies Act 2004

Other documentation which you must check this document against:

- College of Policing – Code of Ethics
- Norfolk and Suffolk Constabularies' Standards of Professional Behaviour
- College of Policing – Authorised Professional Practice

- Norfolk and Suffolk Constabularies' Email, intranet and internet use policy
- Norfolk and Suffolk Constabularies' Mobile Devices policy
- College of Policing – Authorised Professional Practice
- Opinion 2/2017 on Data Processing at Work (EU Article 29 Data Protection Working Party)
- The ICO employment practices code
- Interception of Communications Code of Practice

1. Summary of changes

1.1 This is a new joint Norfolk and Suffolk policy which replaces the 7F policy of the same name.

2. Purpose of Policy

2.1 The purpose of this policy is to outline the circumstances in which Norfolk and Suffolk Constabularies ("the Constabularies") will monitor the use of IT and communications systems.

3. Introduction

3.1 The Constabularies' systems enable the monitoring of telephone, email, voicemail, internet and other communications, for policing reasons, and in order to carry out legal obligations in the Constabularies' role as an employer. Use of the Constabularies' systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Lawful Business Monitoring is the term used within the College of Policing Approved Professional Practice for Counter Corruption to describe the activity of monitoring police ICT systems as detailed within this policy document. Monitoring is only carried out to the extent permitted or as required by law and is necessary and proportionate.

Please note: Monitoring can extend to any use of force communications and data systems, both on and off duty.

4. Aims

4.1 The aim of this policy is to set out how the Constabularies will monitor the ICT devices owned by the Constabularies including desktops, laptops, mobile telephones and other mobile devices. It is intended both to provide policy within which the Professional Standards Department will operate, and to provide information to officers and staff on how data generated in the course of their work may be retained, retrieved, and utilised.

4.2 The specific objectives of this policy are to:

- Put in place mechanisms where wrongdoing by officers and staff can be both proactively and reactively identified through the retrieval of electronically generated data on Constabulary ICT devices.

- Ensure that such mechanisms are used proportionately in order to identify or provide evidence of serious wrongdoing.
- Ensure that appropriate care is taken to protect personal and, in particular sensitive, information which may be entered into Constabulary ICT devices.
- Ensure that the Constabularies' obligations under the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA), the principles of management of police information (MoPI), the Freedom of Information Act 2000 and the Human Rights Act 1998 are complied with.

5. Statement of Policy

5.1 This policy advises officers and staff that monitoring processes are in place and that user activity is recorded and reviewed where necessary, in response to intelligence received or information relating to potential corruption vulnerability, or misconduct, particularly where it presents a risk to the organisations or relates to nationally identified threats. The level of intrusion will be proportionate to the issue being considered and in accordance with the relevant legislation (detailed at the outset of this policy).

5.2 This monitoring will allow the Constabularies to hold officers and staff to account for misuse of force systems, but will also protect officers and staff from malicious complaints.

5.3 Officers and staff should be aware that the primary purpose of Constabulary ICT systems is to conduct policing business, and as such any conversations or other communications using these systems <u>may not be considered private</u>.

5.4 This policy has been formally agreed via the approved policy development/review process. It will be maintained by the Professional Standards Department in conjunction with the Central Policy Unit.

5.5 The policy is intended to promote equality, eliminate unlawful discrimination and actively promote good relations regardless of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation, economic or family status.

5.6 Managers have a responsibility to ensure this policy is applied fairly, and unless otherwise stated, all policies and procedures are non-contractual.

6. Applicability

6.1 Unless otherwise stated, this policy applies to all police officers (including officers of the Special Constabulary) and all members of police staff (including police support volunteers) as well as contractors or third party staff who have access to the Constabularies' ICT Systems.

7. Monitoring

7.1 User activity is recorded by way of automated software ("the Monitoring System").

7.2 Monitoring activity may lead to the interception of a communication, as further confirmed within log on messages on devices and user agreements signed at the time of taking possession of laptops, phones and other mobile devices. In all cases, the level of intrusion must be proportionate to the issue being considered.

7.3 The Constabularies reserve the right to retrieve the contents of e-mail messages, to check internet usage (including pages visited and searches made), Teams chat messages and any other function carried out on the Constabularies ICT systems, as reasonably necessary in the interests of the Constabularies, including for the following purposes (this list is not exhaustive):

- To monitor whether use of the Constabularies' telecommunication systems is legitimate and in accordance with the Constabularies' policies;
- To find lost messages or to retrieve messages lost due to computer failure;
- To assist in the investigation of alleged wrongdoing or misconduct;
- In the interests of national security;
- To prevent or detect crime;
- To secure effective system operation;
- To deliver efficient and effective policing;
- To manage resourcing and expenditure by Constabularies;
- To comply with any legal obligation.

7.4 In particular, the Constabularies may intercept and record communications by way of the Monitoring System in order to:

- establish the existence of facts;
- ascertain compliance with relevant regulatory or self-regulatory practices or procedures;
- ascertain or demonstrate standards which are or ought to be achieved by persons using the Constabularies' ICT systems;
- prevent or detect crime;
- investigate or detect the unauthorised use of the Constabularies' ICT systems;
- ensure the effective operation of the Constabularies' ICT systems.

7.5 Staff and officers are reminded that monitoring can extend to any use of the Constabularies' communications and data systems, both on and off duty. There should be no expectation of privacy when using the Constabularies systems.

8. Circumstances where the Monitoring System may be utilised

<u>Development of information or intelligence received</u>

8.1 Examples may include intelligence received in relation to computer misuse or disclosure of information. This may also include information which has been self-declared, e.g. a disclosable association which has been deemed as presenting a high risk of corruption. Use of the Monitoring System will be on a case-by-case basis.

<u>Complaint and Misconduct investigations</u>

8.2 The Monitoring System can be interrogated to inform PSD or local investigations into Public Complaints, Misconduct or Gross Misconduct. To request interrogation of the system for this purpose, a request should be made to the Detective Inspector of the Anti-Corruption Unit (ACU).

<u>Anti-corruption investigations</u>

8.3 Where the Monitoring System is used as part of an anti-corruption investigation, this should have oversight from an SIO and consideration should be given to any necessary covert authorities / Article 8 compliance as part of the investigation strategy.

8.4 If constant and/or targeted monitoring of a specific officer or staff member using the Monitoring System is required, the ACU Investigator will make an application to the Head of the Professional Standards Department (or deputy in their absence), detailing the necessity and proportionality of the monitoring request. The Head of PSD will then authorise if the necessity and proportionality test is met.

8.5 If the frequency and/or manner of use of the monitoring system would constitute directed surveillance and is likely to infringe on a person's right to a private and family life, then an authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA) should be sought. Any application under RIPA will be considered on a case by case basis by ACU investigators and be authorised in accordance with RIPA and the associated Codes of Practice.

<u>Proactive searching</u>

8.6 The Monitoring System will only be used in this manner to retrieve activity of relevance to PSD's Control Strategy Priorities. Careful consideration will be given to searches in order to minimise irrelevant records returned. Any indication of behaviour contrary to the Standards of Behaviour obtained in this manner will be developed in line with existing ACU intelligence development processes.

Management of potential conduct and corruption.

8.7 The Monitoring System cannot be used for performance management issues, however it can be interrogated to support supervisors in the management of potential corruption/misconduct. Data produced should not be used to assess productivity in terms of work rate; supervisors should be able to assess this through their own record keeping and workflow management. Interrogation of the Monitoring System can be considered where:

- There are specific concerns that an individual is misrepresenting their working hours by mis-reporting start and finish times or not declaring time spent on breaks;
- There are specific concerns about appropriate usage of email, Teams messaging or internet facilities. “Excessive use” will need to be determined by the supervisor in conjunction with other performance data held by the supervisor. PSD will not provide judgements on whether any usage appears excessive.

8.8 To request interrogation for this purpose, a request should be submitted to the ACU Detective Inspector for consideration.

Threat to life/concern for welfare

8.9 There may be rare occasions that the capability of the Monitoring System might present a useful tactical option for a Senior Investigating Officer in a kidnap investigation involving officers or staff or for those managing welfare concerns relating to officers or staff. Requests in respect of such occasions may be made via the ERSOU Sensitive Intelligence Unit or the PSD on-call officer.

Evidential use

8.10 Where possible, data identified using the Monitoring System required for evidential use should then be obtained via a secondary audit of the source system. On occasion, this may not be possible and where data extracted directly from the Monitoring System is required in evidence, authority should be sought from the ACU Detective Inspector. This can then be exhibited in the normal way. If an expert statement is required regarding the functionality of the Monitoring System, this has been agreed as part of the procurement process with the supplier and can be requested via the ACU Detective Inspector.

9. Personal Data

9.1 Searching the Monitoring System may result in the retrieval of data which constitutes Personal Data or Sensitive Personal Data under the GDPR and/or DPA. All officers and staff accessing the Monitoring System have personal responsibility for appropriately managing the information obtained in accordance with GDPR, DPA and the Constabularies’ Data Protection policy. Sensitive Personal Data should be redacted from any data retrieved prior to its use for the purposes outlined above.

10. Subject Access Requests

10.1 Any subject access request for information held by the Monitoring System will neither confirm nor deny whether any ACU investigation has been conducted in relation to specific employees, where the investigation was not previously known to the officer or employee.

10.2 An exemption justifying the rejection of subject access requests will be considered where the grounds are met.

10.3 If requested, a proportionate example of the user's activity will be provided at the discretion of ACU on a case by case basis.

11. Data Review and Retention

11.1 Users of police systems should be reassured that any information obtained and retained by way of the Monitoring System will be handled by officers and staff in ACU, in compliance with the GDPR, DPA and MoPI guidelines.

11.2 Monitoring data will be retained for up to six years and deleted automatically thereafter.

11.3 Monitoring data will be retained in line with the Constabulary retention schedule. Where a specific data type has a retention schedule of less than six years, it will be deleted to comply with the force retention schedule. For example, emails have a retention schedule of two years and so will be deleted from the Monitoring System after two years, unless part of a specific investigation.

11.4 Where data is identified as required for a specific investigation it will be retained and reviewed in line with MoPI guidelines.

11.5 Where inaccurate data is identified in the system it will be deleted.

11.6 The Head of PSD will be the Data Owner/Information Asset Owner for the Monitoring System data held by the Constabularies. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why.

12. Administration and Access

12.1 The ownership and oversight of use of the Monitoring System is located with the Head of Professional Standards.

12.2 Access to the Monitoring System is limited to officers and staff within the Anti-Corruption Unit (ACU), with a minimum vetting level of Management Vetting (MV). Administration of the system will be limited to the ACU Detective Inspector and their designated single point of contact.

Development work will also be carried out by designated single points of contact within ICT.

12.3 The ACU will ensure that those who monitor workers, or who can authorise such monitoring, are briefed on the employer's responsibility under the GDPR, DPA and the ICO (Information Commissioners Office) Employment Practices Code.

12.4 The ACU will have effective systems in place to ensure that passwords and banking details entered on the Constabularies' ICT systems are not compromised by the Monitoring System.

12.5 The ACU will have effective systems in place to ensure that confidential reporting systems to the Professional Standards Department (PSD) are not compromised by the Monitoring System and the author of any confidential reporting to PSD cannot be identified.

13. Audit and Compliance

13.1 Audit of the Monitoring System usage is carried out by dip sample by the ACU Detective Inspector on a monthly basis, to ensure that enquiries are proportionate and carried out in accordance with relevant legislation and policy.

14. Training and Accreditation Requirements

14.1 All officers and staff accessing the Monitoring System will have completed mandatory training in relation to Managing Information, Freedom of Information and Disclosure.

14.2 Training in the use of the Monitoring System is required prior to access, and is delivered by the supplier.

14.3 All officers and staff accessing the Monitoring System have personal responsibility for appropriately managing the information obtained.