Integrity | Professionalism | Fairness | Respect

• Electronic and Telecommunication Systems Monitoring Policy and Procedure

Reference No.	**P12:2003**

Implementation date	**20 February 2003**
Version Number	**1.2**

Linked documents	
Reference No:	**Name.**
P14:2000	Information Security Policy
P13:2001	Internet access and email use procedure
P04:2016	Computer Network Security Operating Procedures
P46:2013	Information Security Incident Management Policy and Procedure

Suitable for Publication	
Policy Section	**Yes**
Procedure Section	**Yes**

Protective Marking
Not Protectively Marked

PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UP TO DATE VERSION CAN BE FOUND ON THE FORCE INTRANET POLICIES SITE.

Table of Contents

1 Policy Section

1.1 Statement of Intent – Aim and Rationale

Dorset Police has a responsibility to protect its integrity and maintain high standards to prevent and detect corruption and to prevent the effects of such behaviour upon the community. It also has a responsibility to protect its staff from corrupt influences and reduce vulnerability of the organisation to such influences. The aim of this policy is to provide Dorset Police with a regulated framework for the lawful monitoring of the activities of its staff, designed to protect the community, Dorset Police and its staff from any wrongdoing emanating from within the organisation.

1.2 Our Visions and Values

Dorset Police is committed to the principles of "One Team, One Vision – A Safer Dorset for You"

Our strategic priority is to achieve two clear objectives:

- To make Dorset safer
- To make Dorset feel safer

In doing this we will act in accordance with our values of:

- Integrity
- Professionalism
- Fairness and
- Respect

National Decision Model

The National Decision Model (NDM) is the primary decision-making model used in Dorset Police. The NDM is inherently flexible and is applied to the development and review of all policy, procedure, strategy, project, plan or guidance. Understanding, using and measuring the NDM ensures that we are able to make ethical (see Code of Ethics), proportionate and defensible decisions in relation to policy, procedure, strategy, project, plan or guidance.

Code of Ethics

The Code of Ethics underpins every day policy, procedures, decision and action in policing today. The Code of Ethics is an everyday business consideration. This document has been developed with the Code of Ethics at the heart ensuring consideration of the 9 Policing principles and the 10 standards of professional behaviour. Monitoring is carried out through the Equality Impact Assessment process which has been designed to specifically include the Code of Ethics.

1.3 People, Confidence and Equality

This document seeks to achieve the priority to make Dorset feel safer by securing trust and confidence. Research identifies that this is achieved through delivering services which:

1. Address individual needs and expectations
2. Improve perceptions of order and community cohesion
3. Focus on community priorities
4. Demonstrate professionalism
5. Express Force values
6. Instil confidence in staff

This document also recognises that some people will be part of many communities defined by different characteristics. It is probable that all people share common needs and expectations whilst at the same time everyone is different.

Comprehensive consultation and surveying has identified a common need and expectation for communities in Dorset to be:-

- Listened to
- Kept informed
- Protected, and
- Supported

2 Standards

2.1 Legal Basis

The Chief Constable has a duty to ensure maintenance of the efficiency and effectiveness of Dorset Police. It is therefore, essential that the necessary procedures and processes are established to ensure that all members of staff are performing the duties required of them to an appropriate standard.

Dorset Police is a public authority and is therefore required to act in a manner, which is compatible with the rights outlined in the Human Rights Act. European case law imposes a positive duty on Dorset Police to prevent crime and protect the rights of others.

The Force has a duty to maintain integrity of its systems and to do so may lawfully intercept staff communications to, prevent or detect crime, to ascertain compliance with policies and procedures and to detect unauthorised use of its business telecommunication systems.
The relevant legislation is contained within:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Telecommunication (Lawful Business Monitoring)(Interception of Communications) Regulations 2000
- Data Protection Act 1998
- Computer Misuse Act 1990

This policy is supplementary to and should be read in conjunction with the following existing Force policy documents;
Force Information Security Policy
Force E-mail and Internet Access (Forcewide Network) Policy
Forcewide Computer Network Security Operating Procedures

2.2 People, Confidence and Equality Impact Assessment

During the creation of this document, this business area is subject to an assessment process entitled “People, Confidence and Equality Impact Assessment (EIA)”. Its aim is to establish the impact of the business area on all people and to also ensure that it complies with the requirements imposed by a range of legislation.

2.3 Any Other Standards

The other standards applicable are shown on pages one and two of this document.

2.4 Monitoring / Feedback

The Information Management Board will be responsible for ensuring the policy is reviewed at 12-month intervals. Additional periodic reviews will be at the discretion of the Board to provide the flexibility to address new vulnerabilities, significant security incidents or significant changes to organisational or technological infrastructures.

The Force Information Security Officer will maintain the policy and provide guidance on its implementation. Amendments or additions to the policy identified by the Information Security Groups will be prepared by the Information Security Officer for formal approval. Audit trails for all policy changes will be maintained through document version control.

Feedback relating to this policy can be made in writing or by e-mail to:

Address: Professional Standards Department, Dorset Police Headquarters, Winfrith, Dorchester, Dorset, DT2 8DZ

E-mail: Complaints & Misconduct@Dorset.pnn.police.uk

Telephone: 01202 - 223881

3 Procedure Section

3.1 Background

Dorset Police provides facilities to its staff primarily for policing purposes and for use in the course of, or in connection with its business. This policy applies to use of;

- The force computer network and the use thereof to access any other system (e.g. NICHE & PNC)
- Other electronic systems not linked to the network and provided primarily for use in connection with business functions of the force. (e.g. “stand-alone” systems and laptop computers, tablets and hand held devices)
- The force telecommunications network and other telecommunication facilities forming part of the force private network
- Other telecommunication facilities provided to staff for primarily business use (e.g. mobile telephones, tablets, hand held devices and pagers)
- Electronic systems provided for purposes of security of buildings (e.g. PAC access)

In the case of the force telephone system, private calls or transmission of private facsimile may be made in appropriate urgent cases, where they cannot be left until the staff member has left work. With regard to e-mail and internet access using force facilities then reasonable personal use is permitted. However with all force systems, they are provided by the force and there can be no expectation of privacy in these communications.

Such Dorset police facilities shall not be used for;

- Unlawful activities
- Personal financial gain
- Personal business interest or commercial purposes
- Activity, which distracts from the routine business of Dorset Police
- Activity expressly prohibited under any other force policy
- Any other activity, which would constitute an act of misconduct

The legislation mentioned above permits Dorset Police to lawfully monitor or intercept communications for legitimate reasons, including;

- Preventing or detecting crime
- Investigating and detecting unauthorised use of telecommunication systems
- Establishing of facts and,
- Ascertaining compliance with policies and procedures in relation to the business of the organisation

Interception authorised under the above Regulations does not apply to mobile telephones or pagers, whether provided by the force or not since they do not comprise a part of the private system. Such monitoring may only be carried out in accordance with the provisions of RIPA. However, monitoring of automated data (e.g. billing data) in respect of telecommunication facilities provided by the force may be subject of monitoring.

Dorset Police expects the highest standards of behaviour from all staff, both on and off duty and that expectation includes honesty, integrity, transparency, fairness, professionalism and self-

discipline. These standards are widely promoted within the force and are reflected in the following documents;

- This policy document
- Statement of Common Purpose and Values
- Force Code of Ethics
- Police Misconduct Regulations
- Conditions of Service for police staff
- Prevention and Detection of Corruption Strategy
- Equal Opportunities Policy
- Grievance Procedure
- Health and Safety at Work
- Human Rights Act 1998

The monitoring of staff is not a new concept. It includes routine supervision of performance and staff behaviour. Recent legal changes extend the principal of supervision into the use by staff of communications equipment provided by the organisation for business purposes.

For the purposes of this policy, “monitoring” means, monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications and includes the recording of anything monitored.

Staff monitoring may engage Article 8, ECHR – the right to respect for private and family life, home and correspondence. However, this is a qualified right in as far as it is recognised that the private acts of individuals can threaten the human rights of others. The organisation is obliged to take action appropriate to the protection of others.

There is also a potential to engage Article 8 by the retention and storage of records created through staff monitoring. See Section 3 – Product of monitoring below.

Failure to comply with any instructions contained within this policy document may result in disciplinary action. Enquiries relating to the implementation of this policy may be made to the Head of Professional Standards.

3.2 Liability to Monitoring

Staff may be liable to monitoring in all aspects of their use of electronic and telecommunication systems provided by or for Dorset Police. Some aspects of monitoring are automated such as;

- Recording of dialled telephone numbers and call duration.
- PNC transactions
- Certain transactions on the Force wide network including NICHE and internet access, e-mail and other systems.
- Automated recording of certain telecommunication facilities, e.g. control room
- Automated recording of access to police premises using the PAC access system.
- Automated recording of itemised billing data received by the force in respect of telecommunications equipment, which is supplied to the individual by the force.

Automated data will continue to be subject of routine monitoring as required under the Data Protection Act and other force policies for management purposes and information security purposes. However, specific monitoring of staff or targeted monitoring will happen neither

continually nor routinely, but will take place as a proportionate response to establish adherence to policy and procedure or to a specific concern or threat to the force. This includes data, which is automated or otherwise. Such specific monitoring shall be authorised only in accordance with this policy and will consider the issues of necessity, proportionality, intrusion / collateral intrusion and likelihood of obtaining private information.

Outside the usual staff / supervisor relationship, unless automated, no technical monitoring of systems use will take place unless authorised in accordance with the procedure outlined in Section 4 below.

Regular circulations will be made, reminding staff of the liability to monitoring.

3.3 Product of Monitoring

Other than product generated by monitoring in accordance with an authorisation under Part 1, RIPA, all material from monitoring will be subject to the provisions of the Criminal Procedure and Investigations Act 1996 and the Data Protection Act 1998.

Section 17 RIPA provides for the exclusion of product from legal proceedings. These provisions do not apply to product generated by staff monitoring on the Dorset Police private system in accordance with lawful business monitoring regulations.

Where it is believed that the product of monitoring could be relevant to pending or future disciplinary or criminal proceedings, it will be retained for an appropriate period. The retention of such material will be subject to periodic review.

3.4 Application and Authorisation process

The monitoring of any system, as specified in 1.1 above must have the appropriate authorisation as shown below.

In the case of any suspected criminal matter, the authorising officer must be the Head of Professional Standards or the Inspector in charge of the Anti-Corruption Unit.

In the case of suspected misconduct of a police officer, the authorising officer must be the Head of Professional Standards or Inspector in charge of Anti-Corruption Unit.

In the case of suspected breaches of police staff discipline code, the authorising officer must be the Director of Human Resources, or Head of Personnel Services.

Applications for authorisation of monitoring will be made in writing on form CA1 and once authorised, forwarded to the force Data Protection Officer or Force Computer Audit Officer. In the case of certain sensitive matters, a copy of the authorisation page only, will be forwarded.

Authorisation as specified in this policy does not apply to the regular routine monitoring as conducted by the Force Computer Audit Officer.

Authorisations will expire after 3 months and it is good practice for the authorising officer to review the authorisation on a monthly basis.

Urgent authorisations may be given by an officer of at least Inspector rank and shall be properly authorised within 72 hours. Urgent authorisations will expire after 72 hours.

Where it is necessary for an authorisation to continue beyond 3 months, an application for renewal must be made on form CA1, which should include an update on the result of monitoring within section 2 of that form.

Where the monitoring no longer meets the criteria for authorisation, it must be cancelled immediately in writing to the authorising officer, who will ensure the monitoring is cancelled by notifying the Data Protection Officer or Computer Audit Officer.

In all cases of monitoring it must be considered whether there is a requirement for any authorisation under RIPA. Where there is any doubt as to whether such statutory authorisation is required the advice of FIB or Professional Standards Unit will be sought. The authorising officer in such cases will be the appropriate Superintendent, who is not involved in the investigation.

3.5 Closed Circuit Television systems (CCTV)

CCTV systems are in use throughout Dorset Police premises for security and crime prevention purposes. Whilst they are not installed for the purpose of monitoring staff activity, product obtained from its use will be made available to management or Professional Standards Unit, where required in connection with any investigation.

4 Consultation and Authorisation

4.1 Consultation

Version No:	Name	Rank/Role	Date
Police & Crime Commissioner			
Police Federation			
Superintendents Association			
UNISON			
Other Relevant Partners **(if applicable)**			

4.2 Authorisation of this version

Version No: 1.2	Name	Rank/Role	Date
Prepared:	J Stephens		19/2/16
Quality assured:			
Authorised:	S Wallbridge		19/2/16
Approved:			

5 Version Control

5.1 Review

Date of next scheduled review	**Date: 22 February 2017**

5.2 Version History

Version	Date	Reason for Change	Created / Amended by
1.0	03112002	Initial Document	
1.1	June 2013	Updated – Fit for purpose review	Johnny Stephens
1.2	February 2016	Updated – Policy Review, fit for purpose review	Sean Walbridge & Bob Lee

5.3 Related Forms

Force Ref. No.	Title / Name	Version No.	Review Date

5.4 Document History

Present Portfolio Holder	Head of Professional Standards
Present Document Owner	Head of Professional Standards
Present Owning Department	Information Security and Assurance
Details only required for version 1.0 and any major amendment ie 2.0 or 3.0:	
Name of Board:	Senior Officers Policy Group
Date Approved:	20022003
Chief Officer Approving:	

Template version February 2016