PS 172 Protective Monitoring Policy

January 2014

Version 2.0

Statement of legislative compliance
This document has been drafted to comply with the general and specific duties in the Equality Act 2010; Data Protection Act; Freedom of Information Act; European Convention of Human Rights; Employment Act 2002; Employment Relations Act 1999, and other legislation relevant to policing.

Table of Contents

Aims and Objectives of the Policy

Nottinghamshire Police, by virtue of Section 6, Human Rights Act 1998, is a public authority and is required to act in a manner that is compatible with the rights outlined in the Convention.

The Regulation of Investigatory Powers Act 2000 (RIPA) enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept or monitor communications for the purposes of carrying on a business. These regulations apply equally to public authorities.

Various legislation and codes of practice including the Data Protection Act 1998, ISO 27001/2 Information Security Management Systems and ACPO Community Security Policy impose a positive duty on the Force to protect its information assets and provide the assurances that appropriate controls are in place.

The monitoring of staff activity is an established concept which includes the routine supervision of performance and staff behaviour. RIPA extends the principle of supervision to the use by staff of communications equipment provided by the organisation for business purposes.

The policy applies to Nottinghamshire Police Officers, Police Staff, Partners, agents and approved persons working for or with the Police

Protective Monitoring is a lawful and ethical tool used to assist the Force in the protection of its staff, information and to assist in the investigation of misconduct or criminal activity. The audit system will monitor and record all computer based actions conducted using any Nottinghamshire Police computer equipment.

This policy defines the monitoring and auditing of staff activity as a means of ensuring all staff comply with Force policy and procedures and with the standards of behaviour expected by Nottinghamshire Police.

This policy does not over-ride any existing policies or negate any existing guidance regarding information security, data protection or acceptable use. It is intended that it will supplement such policies but with a specific focus on the protective monitoring of the force computer network and access to the data held within or transported by it.

Main aims and objectives are:

- To ensure the data integrity of the information held by Nottinghamshire Police and enhance operational security of criminal investigations. This will be achieved by way of a single force-wide network based facility that will audit computer and peripheral device usage independent of any specific application. The system will ensure that Nottinghamshire Police complies with the ACPO Community Security Policy (CSP) requirement to carry out “Protective Monitoring”.

- To identify misuse, monitor exceptional usage and support intelligence led investigations. All users of Nottinghamshire Police LAN accounts must note that the monitoring system will include any personal use staff make of Force equipment, even if undertaken in their own time and with Management agreement. Standard use of all Nottinghamshire Police systems and information is identified to all users as for 'Business Use Only'.

- To provide a forensic capability to the auditing process to ensure its evidential credibility.

- To protect the Force by providing the Counter-Corruption Unit (CCU) with the means by which they can effectively seek out those who abuse their position within the force for personal gain or benefit of others.

- To instil within the communities of Nottinghamshire the confidence that those employed by Nottinghamshire Police maintain the highest levels of honesty and integrity by enforcing the relevant Codes of Conduct in relation to unethical behaviour or gross misconduct.

- To protect the information and intelligence assets of the Force from malicious or accidental disclosure.

Policy Statement

Definitions

Protective Monitoring – The term given to an auditing capability that is network based as opposed to being application specific.

Application – Refers to the software installed on force computers/servers, virtual or otherwise, that will facilitate the logging of actions conducted by the user logged on to a specific terminal or access point.

Console – The administrative and querying interface of the application used to interrogate and manage the system.

Intercept – The "live" monitoring of communications which may involve recording of any activity witnessed.

Monitor – The review of "historic" data recorded and stored within the auditing database.

Communications Equipment – Any equipment that facilitates the creation, transmission or receipt of data provided by the Force and intended for the business use of Nottinghamshire Police.

Ownership

The owner of the Protective Monitoring system is the Head of Professional Standards and is ultimately responsibly for the use of the software application, the information it generates and the maintenance of the Protective Monitoring Policy.

It is the responsibility of the system owner to ensure that any revisions, amendments or alterations to this policy are referred through the corporate decision making process for agreement.

The policy will be subject to annual review by the system owner and be assessed for both privacy and equality impact.

The Protective Monitoring Policy is inextricably linked with the Information Security and Acceptable Use Policies and before any changes are made consultation with the respective policy owners will be undertaken where appropriate.

Administration

The Protective Monitoring data will be stored and controlled by Professional Standards.

The system will be administered by nominated MV/SC vetted CCU staff.

Routine reviews of the audit data will be conducted to ensure compliance with relevant legislation.

Access

Data stored within the Protective Monitoring system will only be accessible to suitably trained members of CCU; access to pre-defined Management Information reports will be available to other Professional Standards staff members as appropriate.

Requests for quantitative/system data must be submitted to the DCI - CCU and each case will be considered on its own merits. Such requests must be made with the authorisation of an officer of the rank of Chief Inspector or above or police staff equivalent.

No personal data will be disseminated outside the department without the explicit instructions of the Department head.

Distribution

All Nottinghamshire Police computers will have the software installed – apart from identified and known exceptions.

All new computers introduced to the force network will be prompted to have the software installed.

Mobile terminals and laptop computers will upload the audit logs automatically on connection to the force network.

Security

The Protective Monitoring data is encrypted at rest on the local machine and during transmission over the force network.

Data stored within the database is afforded the physical and protective security measures required for RESTRICTED material.

Passwords entered by force network users are masked from view. Retrieval of this data is only possible by the software provider who will only conduct the conversion with the authority of a police officer of the rank of Superintendent or above.

All system users and administrators are audited including those with access to the software terminal console.

Policy Publication / System Warnings

A suitably worded logon script will be shown at the point each individual user logs onto a force computer. The text will explain in plain language that access to the force network is for authorised users only and is monitored. Users will be advised that they should have no expectation of privacy if they choose to use the Force computers for personal use. They will also be reminded that personal use must be only be conducted following recorded agreement with Line Management.

All staff will be advised to read the Protective Monitoring Policy which will be made available on the force Intranet.

Attempts to disable/prevent installation or otherwise deliberately interfere with the functionality of the software will be considered a misconduct matter and investigated appropriately. Interference with the system may also constitute an offence under the Computer Misuse Act 1990 and would be treated as a criminal matter.

Information generated by the Protective Monitoring system may be used as grounds for further enquiries and form the basis for further investigation.

The results of audit log interrogation may be used as evidence in misconduct and criminal proceedings.

Data Protection

The Data Protection Act 1998 provides for the regulation of the processing of information relating to individuals, including the obtaining, holding, use and disclosure of such information.

Any information relating to an individual or their actions generated by the audit system will be subject to relevant legislation and protected accordingly.

It is the responsibility of the system owner to ensure that all aspects of the Data Protection Act are complied with.

The requirements for data review, retention and disposal will be applied in accordance with the provisions of the Data Protection Act 1998 and the Management of Police Information (MoPI) Codes of Practice 2010.

Oversight

As part of the implementation process of the Protective Monitoring Policy within Nottinghamshire Police, consultation has been undertaken with the Staff Associations.

The facility will be made to allow the system, processes and users to be independently audited/verified by the Information Security Manager.

Related Documents and Appendices

Documents

Nottinghamshire Police - Information Security Policy

Nottinghamshire Police – Internet and E-mail Use

ACPO - Community Security Policy (CSP)

CESG Good Practice Guide 13 (Protective Monitoring) (RESTRICTED)

Statutory Instruments 2000 No.2699. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Management of Police Information (MoPI) Codes of Practice 2010

Information Security Management Systems (ISO 27001)

References

Police Act 1996

Data Protection Act 1998

Computer Misuse Act 1990

Police (Conduct) Regulations 2012

Public Interest Disclosure Act 1998

Freedom of Information Act 2000 (Law Enforcement)

Police (Complaints and Misconduct) Regulations 2012

Police unsatisfactory performance, complaints and misconduct procedures 2012

Regulation of Investigatory Powers Act 2000

Human Rights Act 1998

APPENDIX 1 – PC Login Screen Wording

New wording for login screen – December 2013 V3.0

Access to the Nottinghamshire Police IT Network is for BUSINESS USE ONLY. You may not use the Force's IT facilities for personal purposes other than where this has been prior authorised in writing by Management and the reason is recorded. You MUST NOT share your log on details with another individual or allow them to use your system access in your absence.

Access to the Nottinghamshire Police IT Network is for AUTHORISED USERS ONLY and is monitored. Consequently, there can be no expectation of privacy if you choose to use the Force's equipment for non-authorised personal use.

National, Regional and Local Force systems that contain police information may only be used for POLICING PURPOSES as defined in the Management of Police Information (MOPI) Guidance as:

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Protection of life and property
- Maintenance of law and order
- Assisting the public in accordance with Force policies and procedures

Any DISCLOSURE of PERSONAL information from Force IT systems to individuals or organisations MUST COMPLY with the DATA PROTECTION ACT 1998 and MUST BE RECORDED. DISCLOSURES of Force data MUST comply with Force Policy and Procedures.

INDIVIDUALS can be LIABLE under CIVIL and CRIMINAL LAW and may face PROSECUTION and/or DISCIPLINARY ACTION where systems are ACCESSED and information VIEWED outside of the Business and Policing Purposes or where information is USED OR DISCLOSED without PROPER AUTHORITY. You must NOT search policing systems in relation to yourself, your relatives or your friends & neighbours or the area where you live, even if you believe that there is a legitimate Policing purpose for this. Where a perceived need arises in these circumstances, you must discuss this with your line manager or the Information Security Manager.

By clicking ok you are accepting and agreeing to adhere to the standards above.

Administration

Version Control

Section changed	Details of change
2.0	**Updated policy**

Monitoring and Review

Measure	Date/period and process of review

Registered Owner

Owner	Author
Head of Professional Standards	Information Security Manager