PROTECT - POLICY

Published | | Event History

Policy owned by People Services

Lawful Business and Internal Monitoring

1. Policy Purpose and key drivers

This policy and its related procedure 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 provide a clear statement as to the extent to which Force systems and assets can and will be routinely 'monitored' and, where there are grounds for doing so, 'intercepted' (as distinct from being routinely monitored), and the levels and limitations of privacy that members of Staffordshire Police and others who use such Force facilities should expect. It also provides an indication of the extent to which Force property, including that allocated for personal use in connection with Force business can be accessed in connection with the aims and purposes of this Policy.

Protective monitoring is a set of business processes, with essential support technology, that are required to be put in place in order to oversee how information communication systems are being used, in order to assure user accountability for the use of those facilities.

Various legislation and codes of practice, including the Data Protection Act 1998, the Employment Practices Code and ACPO Community Security Policy (CSP) 2012 impose a positive duty on the Force to protect its data assets and provide assurances that appropriate controls are in place. Interception and monitoring is one method by which the Force will ensure it complies with these requirements.

The Regulation of Investigatory Powers Act 2000 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. RIPA extends the principle of *supervision* to the use by staff of communications equipment provided by the organisation for business purposes. These regulations apply equally to public authorities.

The policy applies to all members of the Force including special constables, agency staff, and volunteers. It also includes consultants and contractors undertaking work on behalf of the Force and any other person who has the use of Force telephony and communication systems.

<u>Aim, Scope and Purpose</u>

This policy defines what is meant by interception, monitoring and auditing and highlights the associated policies that are used to govern specific system access and acceptable use.

To ensure the data integrity of the information/data held by the Force and to comply with the requirements of the ACPO Community Security Policy (CSP) 2012 to carry out “Protective Monitoring”.

To provide performance and management information in support of business decision making and the maintenance of professional standards of behaviour.

To ensure that staff observe Health and Safety regulations and promote a safe working environment.

To ensure that staff are aware of the extent to which interception and monitoring can and will take place.

To dispel any misapprehension that staff may have regarding the privacy of Force assets.

Monitoring Parameters

Electronic and Manual

Protective monitoring is a set of business processes, with essential support technology, that are required to be put in place in order to oversee how information communication systems are being used, in order to assure user accountability for the use of those facilities.Monitoring will be conducted on all Force assets. It will encompass all data mediums. Technical systems include; the IT network, internal and external email services, internet access, vehicle/equipment movements, CCTV, access controls, internal radios systems, personal digital assistants (PDAs), telecommunications networks and force issued mobile telephones, tablets and smartphones. Manual systems include paper based systems, property systems, file and case management. N.B. Any live interception of Force issued mobile telephones would be subject of a separate application under The Regulation of Investigatory Powers Act 2000 (RIPA)

Members of the Force, others who have the use of Force facilities and members of the public should not expect absolute privacy when using Force telecommunications and electronic communications systems. The only exceptions under this policy are: the use of pay telephones situated within the Force estate, if any are provided .

Interception of Business Communications

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or recipient. Under the regulations, businesses are expected to make all reasonable efforts to inform users that such interception might take place. They allow businesses to intercept communications without consent in the following circumstances:

a) To establish the existence of facts (more likely to be relevant to telephone conversations)

b) To ascertain compliance with regulatory or self regulatory practices or procedures relevant to the business (to ascertain whether the business is abiding by its own policies)

c) To monitor quality control and staff training (but not for marketing or market research)

d) To prevent or detect crime (including such crimes as fraud as well as infringement of IT related legislation such as the Computer Misuse Act 1990 or the Data Protection Act 1998)

e) To act in the interest of national security (in which case only certain specified public officials may make the interception)

f) To investigate or detect unauthorised use of the businesses own communications systems (relevant to potential disciplinary action)

g) To intercept to ensure the effective operation of the system (such as to protect against viruses or to forward e-mails to correct destinations)

h) To gain access to routine business communications (for example when staff are absent on holiday or sick leave)

i) To monitor calls to the businesses welfare or help-lines (subject to conditions)

Environmental
Monitoring within the workplace will encompass physical checks of locations, premises and vehicles controlled by the force for the purposes of Force business.

Extent
Monitoring can and will take place in any and all environments mentioned above. This specifically includes any Force premises, location or storage area that has been adopted for personal use such as lockers, desk drawers, filing cabinets and store rooms, whether secured or otherwise.

No area, location, premises, facilities, equipment or furniture owned or controlled by the Force is exempt from monitoring, no matter how they are being used.

Areas of the Force which hold sensitive details or confidential personal information are subject to this policy. Any monitoring under this policy will only be carried out after careful consideration. Before any monitoring is approved and conducted, due regard will be paid to the nature of the environment to be monitored and the sensitivity of the content which is involved. Monitoring will only be carried out by staff who have the appropriate security clearance.

Physical Searches within the Work Environment
There may be occasions when, in the course of either a misconduct or criminal investigation, reasons of organisational efficiency or health and safety, it is necessary to search Force lockers drawers desks and other areas used for the storage of personal effects. Those utilising such facilities and property provided by the Force should have no expectation of privacy.

In the event of a search being needed, the investigating officer must first attempt to contact the member of staff concerned (unless this would prejudice the investigation) explaining the circumstances. The member concerned will be given reasonable opportunity to be present at the time of the search or nominate another person to attend on their behalf.

At the time of the search, a line manager of the member of staff concerned will also be present. If during the search items are removed the member will be informed as soon as practicable. Once the search is complete the facility will be secured and any damage repaired at police expense.

These procedures may be set aside if the search is being conducted covertly under a RIPA authority.

Authorisation for Monitoring
Please see Lawful Business and Internal Monitoring Procedure.
Authorisation for Interception without Consent
Please see Lawful Business and Internal Monitoring Procedure.

Note

Interception does not include a business accessing a stored collection of e-mails that have been received and opened or deleted by the intended recipient or a business accessing a stored collection of sent e-mails.

Retention of Records

A central record of all authorisations and actions **(Forms LBP and any related reports and documents)** will be maintained by The Force Anti-Corruption Unit. Additionally, the Ant-Corruption Unit will inform the Central Authorities Bureau of any authorisations issued.l These records will be the subject of the appropriate Government Protective Marking Scheme (GPMS) marker and will be treated with the appropriate level of security. They will be retained in accordance with The ACPO Code of Practice on the Management of Police Information (MoPI) and its associated Guidance, and will be retained for a period of at least six years from the date of the conclusion of the authorisation. Consideration must also be given to the provisions of the Criminal Procedures and Investigations Act 1996 regarding disclosure requirements.

LBP 1 - Application for telephone/email monitoring authorisation;
LBP 2 - Urgent authorisation for telephone/email monitoring;
LBP 3 - Authorisation for telephone/email monitoring;
LBP 4 - Cancellation of authorisation of monitoring authorisation;
LBP 5 - Application for renewal of telephone/email monitoring;

Systems Warnings

All staff will be advised to read the policies detailed in this document which are available on the Force Policy Database which can be accessed via the Force Intranet (MySPI)

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 use and 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 conducted in accordance with the Force Information Security Policy (FISP)

The marketing of the Policy will be communicated by a number of methods including; 'Everybody to Everybody' email, 'In Brief' item, Professional Standards blog and during IT courses, aimed at ensuring that all system users are aware of the deployment of system monitoring software on all force computers or terminals and the expectation the force has in them not to misuse systems. All new members of the force will, as part of their induction package, be informed of the Monitoring Policy and its implications.

Human Rights

Staffordshire 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. Those members of the Force working with legal or medical privilege material should be aware of the monitoring of force systems and take appropriate measures to maintain its status.

Article 8 of the Human Rights Act 1998 provides for a right to respect for ones private and family life. Article 8 is a qualified right that applies where there is a reasonable expectation of privacy. This policy makes it clear that there is no Force asset exempt from monitoring and as such no expectation of privacy can exist. This document forms part of a comprehensive communication strategy and is intended to satisfy the notification requirement the force has with regards to Copeland v UK.

The principle of proportionality is inherent in the whole of ECHR legislation and requires that a fair balance is achieved between the protection of an individual's rights and the interest of the community at large. To achieve this any interference with an individual's rights will not go beyond what is strictly necessary to achieve that purpose.

Data Protection

Under the Data Protection Act 1998, the Chief Constable is permitted to collect and use employee data to the extent and standards set out within the Act and accompanying Code of Practice.

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 monitoring or auditing of systems 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 1996 and the Management of Police Information (MoPI) Codes of Practice 2005.

Related Documents	
Links to related documents:	Lawful Business and Internal Monitoring (Procedure)
Gatekeeper - the Author suggested the following Procedure document(s) to link to.	FiSP - Internet and Email Use

Relevant Dates and Review Period	
Effective Date:	06/10/2017
Review Date:	09/10/2018
Review Frequency:	Annually

Policy Basis and Implications

2. Legal Basis:	The legislation which provides the legal basis for this policy is: The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 The Data Protection Act 1998 The Employment Practices Code Article 5(1) of the European Data Protection Directive The Regulation of Investigatory Powers Act 2000 (RIPA) The policy is also introduced in order to achieve compliance with: The ISO 27001/2 Standards for Information Security Management and The ACPO Community Security Policy 2006 which although not legally binding do represent standards of best practice.
3. Management of Police Information (MoPI):	MoPI Policing Purpose: Protecting Life and Property, Preserving order, Preventing the commission of offences, Bringing offenders to justice, Any duty or responsibility arising from common or statute law MoPI Review, Retention and Disposal addressed as follows: Records created under this Policy will be retained for a minimum of six years and will be reviewed by Professional Standards after the lapse of that period or earlier if it becomes necessary to do so.
4. Associated Benefits:	The benefits which will this policy will deliver are as set out above under the paragraphs headed: Aim, Scope and Purpose and Interception of Business Communications. The operation of the Policy will be monitored by the Head of Professional Standards and its success will be assesses against those stated benefits. It will also be assessed in terms of its success in deterring members of the Force from behaving in a manner which is contrary to relevant Force Policy and procedure.
5. Consultation:	Deputy Chief Constable Divisional Commanders and Heads of Support Groups HRMs Head of Professional Standards Head of Anti Corruption Unit Police Authority Head of Information Assurance Team Airwave Director/Head of Information Technology Force ISIT Development Manager Force Information Security Officer Information Assurance Board Occupational Health Manager Force Welfare Officer Unison Police Federation Superintendents' Association Trade Union and Staff Association Meeting (TUSAM) Staffordshire Association for Women in Policing Staffordshire Police Lesbian, Gay and Bisexual Group Staffordshire Police Multicultural Association Staffordshire Police Disability Support Group Staffordshire Police Christian Police Association
6. Financial Implications:	The monitoring activities which will take place under this Policy do present substantial financial and resource implications for the Force due to the equipment which will be required in order to conduct the monitoring and the staff time that will be taken up in carrying out the monitoring. However, these matters have been considered and the necessary finance has been set aside. There are therefore no unforeseen financial implications which are likely to arise from the policy.
7. Human Resources /	Training for members of the Force generally will not be necessary. The

Training:	only training that is required is for those members of staff (Anti Corruption Unit) who will carry out the monitoring and this has already been carried out and financed. If and when there are staff changes or other developments which necessitate further training or refresher training, the required finance will be requested in the annual training budget submissions. Monitoring will be carried out by existing staff and no additional human resources are required by the Policy.
8. Associated Policy:	Force Information Security Policy (FISP) Force Information Security Policy (Internet and email Use) Data Protection - Employment Codes of Practice.

FOI, Human Rights and Equality Impact Assessment Indicators

FOIA:	Release to Public		
ECHR:	Compliant with proportionality test	Articles engaged:	Article 8 Right to respect for Private and Family life
EIA:	Compliant	Compliant with Code of Ethics:	Yes

Indexing

Categories:	Anti Corruption Unit

PROTECT - POLICY