Security of local databases and information held on the PNC (West Midlands Police)

(1) Who you are and a brief summary of your career history.

I am currently Chief Constable of West Midlands Police having held that post since June 2009. I have 31 years service in the police having joined the Metropolitan Police in 1980. I held the post of Chief Constable of Staffordshire Police between September 2007 and June 2009 and was Deputy Chief Executive of the National Policing Improvement Agency between 2006 and 2007.

In addition to my duties within West Midlands I hold the ACPO portfolio on Forensic Science. I am Vice Chair of the Counter-Terrorism Committee and chair a joint Police/Government group on Bureaucracy in Policing.

(2) Please identify the databases, owned and operated by West Midlands Police, that hold personal/private information relating to individuals, for example the local intelligence database. In respect of each database please explain (i) what broad categories of information are held on it; and (ii) who has access to it and for what purposes.

i) The list of applications that hold personal information is enclosed at **Annex A**. Each application has a 'System Owner' who is responsible for maintaining a System Operating Policy (SysOps) document that details information management arrangements including roles & responsibilities; the GPMS value of information assets and purpose for which data is held; handling & disclosure: etc. in line with British Standards BS7799 & BS27001.

ii) The categories of information that may be held on WMP force systems as notified to the Information Commissioner are-

- Personal Details
- Family, Lifestyle and Social Circumstances
- Education and Training Details
- Employment Details
- Financial Details
- Racial or Ethnic Origin
- Political Opinions
- Religious or Other Beliefs Of A Similar Nature
- Physical or Mental Health or Condition
- Sexual Life
- Offences (Including Alleged Offences)
- Criminal Proceedings, Outcomes and Sentences.
- Physical identifiers including dna, fingerprints and other genetic samples.
- Sound and visual images.
- Licenses or permits held.
- Criminal intelligence.
- References to manual records or files.
- Complaint, incident and accident details

The organisations that WMP may obtain information from and may disclose information to as notified to the Information Commissioner are:

- Law enforcement agencies.
- Regulatory bodies
- Licensing authorities
- Legal representatives
- Prosecuting authorities
- Courts
- Prisons
- Security companies
- Partner agencies involved in crime and disorder strategies.
- Private sector organisations working with police in anti-crime strategies.
- Police authority
- Emergency services
- Voluntary sector organisations.
- Approved organisations and people working with police.
- Data subjects themselves
- Relatives, guardians or other persons associated with the data subject
- Current, past or prospective employers of the data subject
- Healthcare, social and welfare advisers or practitioners
- Business associates and other professional advisers
- Employees and agents of the data controller
- Persons making an enquiry or complaint
- Police forces
- Local government
- Central government
- Voluntary and charitable organisations
- Ombudsmen and regulatory authorities
- The media
- Data processors

Being in the list does not remove the need to ensure that any disclosure is justified; auditable; proportionate; accountable and necessary.

(3) How does information get placed on those databases? Who decides whether the information should be inputted?

Data is input by authorised users of the system, the system's administrator and the system 'Owner' decide what information is to be held on the system.

As an example the force's intelligence database can have entries initiated by many officers. These entries are submitted to trained intelligence staff that then review, sanitise and ultimately input the appropriate intelligence into the system.

(4) How do users access the databases?

The input of data is completed via the source systems as above and similary, users can view data in each system, however, once entered much of it is exported to a warehouse database where it can be searched and viewed by two systems – Corvus and Flints.

Access is controlled once staff are suitably authorised to use the system by two factor authentication – a Smartcard and a PIN.

(5) How is access to those databases restricted and controlled? The Inquiry is interested in both technical and non-technical measures (such as instructions to users).

Access to the force domain (an essential first step to access other systems) is given only to those that -

- Have passed a security check;
- Have completed their on line data protection training; and
- Have completed their on line GPMS training

Access to systems is controlled by a user's privilege level in accordance with their role. The system 'Owner' for a system decides who shall have access rights to that system. Part 1 Order 67/2005 sets out the overarching Operating Rules for all police information systems and is enclosed at **Annex B.**

Access to Flints is only given to those that have completed the training. Enclosed at **Annex C** – "Access to Flints" shows the information placed on the force's intranet site.

Corvus access is managed by staff being put into the necessary Authorised Data (AD) groups and based on their roles as described in the HR system. The enclosed **Annex D** -"Access to Corvus", shows the information placed on the force's intranet site.

(6) What systems and/or measures are in place to ensure that information held on the databases is not misused? The Inquiry is interested in both technical and nontechnical measures.

An 'Acceptable Use Statement' is presented at the point of logon to all users and is enclosed at **Annex E**. The user must read the statement and agree to the terms of use by first clicking to confirm before access can proceed. Systems include an additional warning before their logon screen, in that they must be authorised to use the system and unauthorised use is potentially a criminal offence. Systems have audit facilities in place that can trace users' activity on the systems. The Forces' Professional Standards Department (PSD) team proactively monitor and investigate potential misuse.

Training is given for access to systems and all users must complete their on-line data protection training before being able to log on to the force network.

Extracts of training material for Flints and Corvus are enclosed at **Annex F**.

(7) Are individual users subject to any vetting procedures or security checks? If so, please give details. Is there a system in place for monitoring and reviewing the suitability of a person to have continued access to the databases? If so, please give details.

All users are vetted under the ACPO/ACPOS Police National Vetting Policy. All users are required under force policy to immediately report any change that might affect their current vetted status. More sensitive staff roles which give greater systems access require additional vetting.

Unused logons are disabled after a period and will only be re-enabled with appropriate evidence that access is still required and where appropriate further training provided.

(8) Are any restrictions placed on an individual user's ability to access information held on the databases (whether by technical means or by way of instructions to the user)? For instance, do some users have greater access rights than others? If so, describe the levels of access and to whom they apply respectively.

All access to data is subject to 'need-to-know' and according to role/responsibility, and access privilege is granted accordingly. This is underpinned by Part 1 Order 67/2005 sets out the overarching ACPO/ACPO Operating Rules for all police information systems.

Access permissions are administered by a central Service Desk and subject to appropriate authorisation by business and system owners that vary from system to system. A new Public Key Infrastructure authentication system ('Gateway') is being implemented that requires a Smartcard and PIN to provide access to force systems.

(9) Are individual users permitted to browse the information to which they do have access without restriction? If not, what restrictions are in place and how are they communicated to individual users?

Data from police information systems may only be directly accessed by serving police officers and police staff who, in order to carry out their official duties require access to the data. Part 1 Orders 67/2005 and 06/2010 Roles and Responsibilities in relation to Police Information Systems are enclosed at **Annex G**. Systems can be audited for potential misuse.

(10) What training is provided to individual users of the databases to ensure that they understand what is and what is not lawful/appropriate use of the information held on the databases? Who is responsible for providing this training?

Users are provided with comprehensive eLearning training covering their Information Security and Data Protection obligations. A minimum test score of 70% is required as a prerequisite for granting access to police information systems. Some force systems however require further training of staff and they must pass this training before they are authorised to use it i.e. FLINTS. Training is provided by either Leadership & Training Centre Tally Ho! or by dedicated training officers within force regional training hubs.

(11) What systems and/or measures are in place to audit the use of the databases by individual users? Describe the system of auditing, if any, that is in place.

Each system 'Owner' has responsibility for the regular audit of users and their access. Information management obligations, together with audit processes and procedures should be fully recorded within the 'SysOps' document for each system.

Audit is risk based and proportionate to the specific systems. Those systems which are high risk are overtly and covertly audited.

(12) What systems and/or measures are in place (i) to prevent; (ii) to detect and (iii) to deter individual users of the databases from unlawfully disclosing information?

(i) The West Midlands Police Counter Corruption Unit (CCU) engages in a variety of different measures to prevent, detect and deter individuals from unlawfully disclosing information. This can take the form of environmental scanning of press and social media and close liaison with crime SIO's to verify what should be in the public arena - guarding against inappropriate reporting of information.

The CCU has confidential reporting options available to staff to report concerns and also has an IT system dedicated to proactively monitoring WMP systems and databases. These IT tools can retrospectively gather information if unlawful disclosures are later reported and have in the past been used to successfully prosecute staff who have committed criminal offences.

The Counter Corruption Unit capability also includes CHIS handling and covert surveillance. All intrusive options would have to satisfy RIPA legislation or lawful business monitoring authorities with regards the necessity and proportionality of the intended action.

(ii) System 'Owners' are required to regularly monitor user access and to ensure that all users of their system fully understand their obligations as detailed in the ACPO/ACPOS Information Systems Operating Rules. System users are made fully aware of the consequences attaching to misuse and abuse of official systems and are required to report any suspicions or irregularities.

(iii) The force has an Incident Reporting system to capture issues such as unlawful disclosure enclosed at Annex H. Any breaches of data protection are also notified to the ICO

(13) Do you consider that the systems and/or measures referred to in question (12) above work effectively? What changes, if any, do you consider should be made to them?

Current monitoring and audit systems do work effectively but do need regular maintenance and scrutiny to ensure our capacity and capability remains at full strength.

Compared to the volume of daily legitimate PNC transactions and lawful systems access across the organisation, the unlawful access to and potential disclosure of information is not a regular occurrence.

However, the prevention and detection of internal threats from employees with legitimate access to force systems remains a priority and methods to prevent and detect such activity are always evolving.

Awareness and preventative work has been led by the Professional Standards Department and future Workstreams under consideration include the creation **of a** dedicated Proactive Monitoring Team to modernise and consolidate audit and monitoring systems in ICT and Counter Corruption under one team.

(14) In the last 5 years:
a. How many suspected unlawful disclosures have there been of information held on the databases to the media and/or private detectives?
b. How many investigations have there been into those suspected unlawful disclosures of information? What was the outcome of those investigations?

Year	Investigations	Leak Identified?	Outcome
2007/08	0		
2008/09	1	Yes	NFA
2009/10	3	Yes x3	1 x Written Warning 2 x NFA
2010/11	6	Yes x3 No x3	4 x NFA 1 x Management Action 1 x Ongoing
2011/12	5	Yes x4 No x1	2 x Ongoing 3 x NFA

The enclosed **Annex i** “examples of leaks” gives more details on this.

All of the 15 cases above relate to information disclosed to the media. Over this time period there have been no investigations related to unlawful disclosure to private investigators. The inappropriate or unlawful disclosure of information in these cases can come from a number of sources. Police databases are the predominant source in the majority of cases.

Disciplinary action in relation to media leakage is detailed above (Written Warning, Management Action etc). All other cases relate to disclosure of information to friends, family, 3rd parties or criminal associates.

As a comparison, over the same time period there were 354 investigations conducted into inappropriate information disclosure to family, friends etc. Three officers have been imprisoned, a further 6 convicted at court and 19 have resigned whilst under investigation.

Since the Police (Conduct) Regulations 2008 came into force, 2 officers have been dismissed and 2 officers have received Final Written Warnings. Other outcomes include Management Advice (12), Written Warning (5) and No Further Action (236).

(15) Do you consider that the unlawful disclosure of information from the databases is a current problem? Please explain your answer.

Considering the volume of daily legitimate transactions carried out by WMP staff using databases, the actual level of misuse is minimal. When there is evidence of misuse of information held on databases then the matter is referred to the Counter Corruption Unit, thoroughly investigated and referred to both criminal and misconduct proceedings.

(16) As regards the personal/private information held on the Police National Computer, what role does West Midlands Police play in preventing, detecting and deterring its personnel (both police officers and civilian staff) from unlawfully disclosing such information? Please describe the systems and/or measures in place (both technical and non-technical).

PNC as a national system is subject to the PNC Code of Connection which all forces are obliged to comply with. A local PNC Auditor tool is in use for the purpose of preventing, detecting and deterring unlawful disclosure. There is mandatory training for any officer before access to PNC is given. This includes the handout of a security reminder (PNC Reminder Handout).

The level of what can be viewed is set on a need to know basis and is only given to those who have completed and passed the appropriate training.

Physically the terminals are only permitted to be installed in appropriate locations, authorised by the Force PNC Manager.

Additional security measures such as screen filters are put in place in offices that are shared with partner agencies to prevent PNC data being seen by non authorised people. In addition the movement of force computers with PNC access is managed and authorised by the PNC Manager. The system is such that each request for information taken from PNC by an officer there is a data-line which requires: Reason Code, Officer Requesting (Name & Collar Number) Date and Time.

(17) What training is provided to individual users of the PNC to ensure that they understand what is and what is not lawful/appropriate use of the information held on the PNC?

The training is modular and all officers must at least complete the initial package before being granted access. This package is enclosed at **Annex J** (Intro to PNC May 10v7 book), attention is drawn to pages 8-10 which cover data protection in detail. Only those officers/staff that provide information to operational staff are trained to use PNC. There is a central PNC Bureau team that input PNC updates for the force.

(18) What systems and/or measures are in place to audit the use of the PNC by West Midlands Police personnel? Describe the system of auditing, if any, that is in place.

WMP have installed an automated electronic auditor (Lynx Auditor) that emails details of checks carried out by a person to the individual's line manager or supervisor to ensure the check was necessary, proportionate and relevant. Guidance and training presentation enclosed at **Annex J.**

(19) Do you consider that the systems and/or measures referred to in question (18) above work effectively? What changes, if any, do you consider should be made to them?

Roll out of the Lynx Audit system is currently ongoing and will be fully deployed across the force has been by September 2012.

(20) In the last 5 years:
a. How many suspected unlawful disclosures have there been of information held on the PNC by West Midlands Police personnel to the media and/or private detectives?
b. How many investigations have there been into those suspected unlawful disclosures of information? What was the outcome of those investigations?

- Question 14 gives information regarding suspected unlawful disclosures (in the last 5 years) in relation to the media and private detectives. A majority of the conduct investigations relate to officers accessing FLINTS inappropriately or unlawfully. FLINTS is a WMP intelligence database that holds information from PNC as well as restricted and sensitive information from other databases.

- It is not possible to separate the number of investigations that related solely to access to the PNC as in the majority of cases officer's access PNC data via the FLINTS database.

(21) Do you consider that the unlawful disclosure of information from the PNC by West Midlands Police personnel is a current problem? Please explain your answer.

- Considering the volume of daily legitimate transactions carried out by WMP staff using the PNC, the actual level of misuse is minimal. When there is evidence of misuse of PNC or any other intelligence database then the matter is referred to the Counter Corruption Unit, thoroughly investigated and referred to both criminal and misconduct proceedings.

(22) Were changes made to any policies, procedures or systems relating to use of the databases and the security of the same following Operations Motorman, Glade and Reproof? If so, please specify.

I don't believe so.

(23) What additional measures, if any, should be put in place to prevent the unlawful disclosure of information held on the PNC and West Midlands Police's own databases?

- Our current proactive capacity and capability is good. A dedicated proactive monitoring team is a consideration that will bring together different audit and monitoring tools currently used within different departments (ICT and Counter Corruption). Our aim is to blend audit regimes in information security with counter corruption technology to monitor and detect suspicious activity.

The documents you should provide to the Inquiry Panel are:
(a) Documents recording the systems and measures referred to above (limited to the
last 5 years);
(b) Instructions/guidelines for users of the databases (limited to the last 5 years).

Signed Chris Sims OBE QMP DL
Chief Constable
West Midlands Police