Police Federation
of England and Wales

Ffederasiwn Heddlu
Lloegr a Chymru

Established by Act of Parliament

Federation House, Highbury Drive, Leatherhead, Surrey KT22 7UY
Telephone 01372 352000 Fax 01372 352044
www.polfed.org

FROM THE DEPUTY GENERAL SECRETARY'S OFFICE

SS/sg

26 October 2010

JBB CIRCULAR NO : 030/2010

To: The Chairman and Secretary
All Branch Boards
Discipline Liaison Officers

Dear Colleagues

APPLICATIONS FOR CRIMINAL / MISCONDUCT ADVICE IN RELATION TO THE USE OF POLICE COMPUTER SYSTEMS FOR A 'POLICING PURPOSE'

Police Officers are in an extremely privileged position in that they have access to both the Police National Computer (PNC) and Force Intelligence Systems on a daily basis. Many requests for legal assistance are received from members who have been served with Regulation 15 notices in relation to their use of police computer systems.

In an effort to get a clearer understanding of what constitutes and what does not constitute a "policing purpose" in connection to any checks of police computer systems, advice has been obtained from Russell Jones & Walker.

Chief Officers are authorised to retain, control and use data for a "police purpose". **This essentially means the investigation, detection and prevention of crime**. Whilst almost all police officers can access police computer systems for an authorised purpose, there have been many examples of officers accessing systems for a non authorised purpose. This Circular is therefore intended to give some guidance on what is a non authorised purpose.

Officers who access computer systems for a non authorised purpose are liable to be prosecuted for the criminal offences of 'unauthorised access' under section 1 Computer Misuse Act 1990 or obtaining or disclosing or procuring the disclosure of data for a 'non authorised purpose' under section 55 Data Protection Act 1998.

Offences of this nature can be punishable with imprisonment. Officers are also liable to face misconduct proceedings for failure to meet the appropriate standards of 'confidentiality' or 'orders and instructions' and these can be assessed as gross misconduct.

Generally, an authorised purpose is the investigation of crime. However, it would be a mistake for a police officer to conduct or request a check on a police computer system in any matter that related to them personally, without first obtaining the approval of a line manager.

For example, conducting a vehicle check on a vehicle registered to a neighbour, or on a vehicle registered to an estranged partner's new partner, or accessing a crime report in relation to a friend, who has been a victim of crime, are likely to be viewed as checks for personal reasons and not for a legitimate police purpose.

The reported case of DPP v BIGNALL [1998] 1 Cr. App. R 1 suggests that if a police officer has general authority to access police computer systems he does not commit the offence of *unauthorised access* contrary to the Computer Misuse Act. However, in this case the Divisional Court made it clear that the officers could have been prosecuted under the Data Protection Act or dealt with under the police disciplinary proceedings.

This was confirmed in the later House of Lords case of R V Bow Street Magistrates Court Ex p. Allinson (No.2) [2000] 1 Cr. App. R. 61 which additionally said that the fact that a police officer had a general authority to access police computer systems did not mean that he had authority to access for a non authorised purpose.

Most Forces have issued internal standard operating procedures (SOPs) which define the limits of a police officer's authority to access police computer systems. Any departure from these SOPs is likely to be viewed as a non-authorised purpose which could result in the officer being prosecuted or disciplined. Officers should familiarise themselves with their Force's SOP. However, the best advice is that if there is any doubt as to whether a particular check is authorised or not, an officer should obtain the approval in writing of a line manager before conducting any such check.

'Police Friends' should be careful in relation to conducting any checks in the preparation of the defence on behalf of an officer facing investigation or proceedings. Friends will be aware of the penultimate paragraph of page 9 of the Home Office Guidance on Police Misconduct, Unsatisfactory Performance and Attendance Management Procedures which provides guidance on the role of the *friend* and states

...It is not the role of the friend to conduct his or her own investigation into the matter...

Whilst R v Chief Constable of The North Wales Police force ex parte CONNAH (which is in the Police Federation Conduct Manual 2008) confirms that a friend is entitled to prepare the accused officer's defence, including the interviewing of witnesses without the interference of the Force or the investigating officer, it would not be appropriate for the friend to conduct checks on the police computer system to ascertain whether a complainant or witness was 'known to police'.

Paragraph 351 of the IPCC Statutory Guidance (April 2010) also confirms the Information Commissioner's view that a routine enquiry on the PNC for any previous convictions of a complainant is a breach of the data protection principle that information should be used for the purpose for which it was collected, i.e. the prevention and detection of crime.

As such information would be a matter of record; the appropriate course would be to invite the investigating officer to conduct such checks under the Guidance paragraph 2.117. This would protect the friend from any suggestion that this was an unauthorised access.

From the research conducted it can be concluded that there is very limited legitimate access to police computer systems and if the access is not in relation to **the investigation, detection or prevention of crime** then that access will be deemed as for a non authorised purpose.

To further emphasise the seriousness of non authorised access, a recent crown court case involved an officer who accessed a force intelligence system in relation to checks on their and an ex-partners motor vehicle. This access resulted in several charges of 'Misconduct in a Public Office' and a subsequent sentence of 9 months imprisonment suspended for 2 years.

In sentencing the officer the Judge said;

"In the modern world it is axiomatic (self evident/obvious) the police must hold huge amounts of information about all citizens.....It is vital we all have confidence in its safekeeping and those who have access to it.

Any misuse of that access by a public servant brings the system into disrepute. It undermines the trust the public may have in the police"

This gives a clear warning to members of the seriousness in which non authorised access of police computer systems is viewed and it is essential that if any member has a doubt about the validity of a particular check, they should seek guidance and authority from a supervisor or manager before carrying out such a check. If authority is not given then the member should not carry out the check.

This needs to be borne in mind when assessing requests for legal assistance in accordance with the 'Funding Criteria' as although any checks may have occurred whilst the member was on duty, if they have not been conducted for an authorised purpose as outlined above, then they cannot be construed as being in the performance or purported performance of their duties as a member of a police force and therefore funding for legal advice and/or representation is likely to be refused.

The contents of this circular need to be clearly emphasised and brought to the attention of the wider membership.

If you have any queries with regard to this circular, please do not hesitate to contact me.

Yours sincerely

STEPHEN A. SMITH
Deputy General Secretary