Durham Standard MAY 2011

WHAT IS A 'POLICING PURPOSE'?

Chief officers are authorised to retain, control and use data for a "policing purpose". This essentially means the investigation, detection and prevention of crime. While almost all staff can access police computer systems for an authorised purpose, there have been many examples of our staff accessing systems for non-authorised purposes.

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

Offences of this nature can be punishable with imprisonment. The individual is also liable to face misconduct proceedings for failure to meet the appropriate standards of either confidentiality, or under 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 staff member 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 is likely to be viewed as checks for personal reasons, and not for a legitimate police purpose. Just because an individual has general authority to access police computer systems, this does not preclude them from committing offences under the Data Protection Act. A recent House of Lords case stated that the fact that a police officer had the general authority to access police computer systems did not mean that they had authority to access them for a non-authorised purpose.

It is clear from relevant research that there is a very limited legitimate access to police computer systems, and if the access is not in relation to the investigation, detection or prevention of crime, and fits with your role, then such access will probably be deemed as for a non-authorised purpose. Just to emphasise the seriousness of non-authorised access, a recent case involved an officer who accessed a force intelligence system in relation to checks on their and an ex-partner's motor vehicle. This access resulted in several charges of misconduct in a public office, and a subsequent sentence of nine months imprisonment suspended for two years.

The judge in the case commented, "In the modern world it is axiomatic (self evident / obvious) that the police must hold huge amounts of information about all citizens". It is vital we all have confidence in its safe keeping, and those who have access to it. Any misuse of that access by a public servant brings the system into disrepute and undermines the trust the public may have in the police.

This should give a clear warning to all members of Durham Constabulary of the seriousness in which non-authorised access of police computer systems is viewed. It is essential that if any member has any 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 you should not carry out the check.