ADVICE ON USE OF POLICE COMPUTER SYSTEMS

Members should familiarise themselves with the Police Scotland Data Protection SOP. It defines the limits of a police officer's authority to access police computer systems. Any departure from the terms of this SOP could result in a member being prosecuted or disciplined.

Chief Officers are authorised to retain, control and use data for a "police purpose". The Data Protection Register entry for the Chief Constable provides some guidance as to the meaning of policing purpose: *"The prevention and detection of crime; apprehension and prosecution of offenders, protection of life and property; maintenance of law and order; also rendering assistance to the public in accordance with force policies and procedures."*

Officers who access computer systems for an unauthorised purpose may be prosecuted for criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 1998 or indeed both or indeed common law e.g. perverting or attempting to pervert the course of justice. In addition, officers making unauthorised use of systems could be subjected to conduct proceedings.

Unauthorised uses might include 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. These examples would be viewed as checks for personal reasons and not for a legitimate police purpose. Courts have held that while some of these checks may have been carried out for a humanitarian purpose they were not for a policing purpose.

BEST ADVICE IS that if in doubt – check with a supervisor. Similarly, if during an investigation an officer stumbles across data that could be deemed personal then – record the incident in the police notebook and inform a supervisor immediately.

In any particular case, officers should contact an SPF Conduct Representative for advice as soon as possible.