



POLICY	Issue 3.0
ACCESS AND DISCLOSURE RELATING TO INTELLIGENCE AND INFORMATION SYSTEMS	10/02/2011

Policy Statement

The Civil Nuclear Constabulary (CNC) has access to a number I.T. systems / databases where information and intelligence is stored. These include national systems e.g. the Police National Computer (PNC), the Scottish Criminal History System (SCHS), stand alone access to proprietary systems such as the National Register of Electors and secure CNC specific systems such as the CNC Intelligence System (CIS). Access to such data is necessary in support of law enforcement activity, national security and the protection of nuclear licensed sites and nuclear material.

These databases contain information and intelligence relating to persons, vehicles and certain types of property and are available to all CNC Police Officers in connection with their official duties (including Escorts Operations and external patrols). The data may be accessed without reference to a supervisor. Some data is also available to HR Officers in connection with recruitment vetting checks.

The CNC will put into place processes, procedures and guidance to users and supervisors to enable authorised persons to access the data contained in these information and intelligence systems and to ensure, as far as reasonably possible, that:-

- unauthorised access is prevented;
- data is protected against improper use or disclosure;
- access accords with system operating instructions, security operating procedures and training provided.

Aims of the Policy

The aims of this policy are to ensure, as far as reasonably possible, that information and intelligence contained in I.T. systems / databases to which CNC Police Officers and Police Staff have access:-

- is properly authorised and necessary in support of law enforcement, national security and the protection of nuclear licensed sites and nuclear material;
- is protected against improper disclosure through appropriate processes; procedures, audits and supervision
- is processed and handled in compliance with legislation, codes of practice and national guidance documents.

This policy is enacted by the following management system documents:

CNC/POL/2.3 Security Policy

CNC/POL/2.3.1 Data Protection Policy

CNC/PP/0061 Access and Disclosure Relating to Intelligence and Information Systems

Document Reference	CNC/POL/17.1	Page 1 of 1
Uncontrolled when printed unless subject to controlled issue. Refer to Policies Index for current version.		

Policy produced from Template:	CNC/CD/0391 CNC Policy Template	R 7.0
--------------------------------	---------------------------------	-------