



G669

## **POLICY FOR INFORMATION SECURITY**

Nottinghamshire Police is committed to ensuring that the information it stores and processes is subject to appropriate security measures whose aim is to provide:-

- Confidentiality: ensuring that information is accessible only to those who are authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and of information-processing methods; and
- Availability: ensuring that authorised users have access to information and associated assets when required.

Measures have been put in place to address internal and external threats to the information and information assets for which the Force is responsible. These include physical, electronic, personnel and procedural controls. Existing security measures and the threats faced by Force information and information assets are under continuous review, to enable additional or more appropriate measures to be applied when necessary.

The strategic and operational approaches to Information Security Management that have been taken by the Force have primarily been designed to comply with the ACPO Community Security Policy. Other policies and directives that are incorporated into the Force's information security strategy include: the Government Protective Marking Scheme; the National Vetting Policy for the Police Community; and the ACPO Manual for Data Protection Management. Cognizance is also taken of the requirement to apply measures that comply with, and uphold UK law. In this respect, particular attention is paid to legislation that specifically relates to information, such as the Data Protection Act 1998 and the Computer Misuse Act 1990.

Author: \_\_\_\_\_ Date: \_\_\_\_\_

Mark Weston  
Information Security Manager

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

Steve Green  
Chief Constable

This policy should be read in conjunction with the appropriate Force Policies, Procedures, Guidance and Rules outlined below: -

PD 22A	Airwave System Security Procedure
PD 094	E-Mail Procedure;
PD 137(1)	Information Security Procedure: Part 1 – General Conditions Use of Privately Owned Equipment for Force Purposes (Appendix B of Information Security Policy: Part 1); Access to Personally Assigned and Shared Drives on Force IT Systems (Appendix C of Information Security Policy: Part 1).
PD 137(2)	Information Security Procedure: Part 2 – Management Requirements;
PD 140	Internet Usage Procedure; Spectrum System Security Policy Spectrum Security Operating Procedures External Network Connections Accreditation Document Set