



POLICY	Issue: 1.0
Management of Digital Evidence	Date: 15/03/2011

1 Policy Statement

1.1 The Civil Nuclear Police Authority (the Authority) and the Civil Nuclear Constabulary (the Constabulary) has approved the introduction of the processes which create and preserve digital forensics evidence so that such evidence can be analysed to support and investigation in the future. This policy, more commonly referred to within Government as the 'Forensics Readiness Policy', should maximise the potential to use digital evidence whilst minimising the costs of investigation. This decision reflects the high level of importance placed upon minimising the impacts of information security events and safeguarding the interests of both the Authority and the Constabulary.

2 Aims of the Policy

2.1 This policy has been created to;

- protect the Authority and Constabulary, its staff and contractors through the availability of reliable digital evidence gathered from its systems and processes;
- allow consistent, rapid investigation of major events or incidents with minimum disruption to Authority and Constabulary business;
- enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required; and
- demonstrate due diligence and good governance of the Authority's and Constabulary's information assets.

3 Background

3.1 The management of digital forensics evidence is required to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required in a formal dispute or legal process. In this context, digital forensics evidence may include evidence in the form of log-files, emails, back-up data, removable media, portable computers, network and telephone records amongst others that may be collected in advance of an event or dispute occurring.

3.2 The production of digital forensic evidence can support a legal defence, it can verify and may show that due care was taken in a particular transaction or process, and may be important for internal disciplinary actions.

Document Reference	CNC/POL/2.3.5	Page 1 of 4
Uncontrolled when printed unless subject to controlled issue. Refer to Index of Policies for current version		

Policy produced from Template:	CNC/CD/0428 CNPA Policy Template	R 5.0
--------------------------------	----------------------------------	-------

3.3 In certain situations digital evidence may be required in a formal investigation. An investigation of this type may require to be launched in the following situations:

- **Security incidents:** unauthorised access to, tampering with or use of IT systems, electronic attack, including denial of service and malicious software ('malware') attacks (viruses, worms, trojan horses);
- **Criminal activities:** fraud, deception, money laundering, threats, blackmail, extortion, harassment, stalking;
- **Commercial disputes:** intellectual property rights;
- **Disciplinary issues:** accidents, negligence, malpractice, abuse of acceptable use policy, grievance procedures;
- **Privacy issues:** identity theft, invasions of privacy, non-compliance with the Data Protection Act and other relevant legislation.

4 Responsibilities

Senior Information Risk Owner (SIRO); The SIRO is responsible for coordinating the development and maintenance of procedures to implement this policy and standards for the Authority.

Security Manager; The Security Manager is responsible for the ongoing development and day-to-day management of this policy within the Authority's overall Risk Management Strategy and additionally will ensure that through Staff disciplinary investigations, all digital evidence forensic readiness procedures carried out are in line with the procedures laid down within Disciplinary Procedure: Police Staff: CNC/PP/0413 and the ACPO Good Practice Guide for Computer Based Electronic Evidence

Head of Professional Standards; The Head of Professional Standards will ensure that where required through misconduct investigations, all investigations requiring digital evidence are carried out are in line with the procedures laid down within Police & Conduct Regulations 2008: Police Officers; procedure 'CNC/PP/0027 Police Officer - Misconduct' and the ACPO Good Practice Guide for Computer Based Electronic Evidence.

Document Reference	CNC/POL/2.3.5	Page 2 of 4
Uncontrolled when printed unless subject to controlled issue. Refer to Index of Policies for current version		

Policy produced from Template:	CNC/CD/0428 CNPA Policy Template	R 5.0
--------------------------------	----------------------------------	-------

5 Definitions

5.1 Key definitions are:-

- Digital forensic evidence readiness

The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.

- Digital forensic evidence planning

Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence, related monitoring and collection processes and capabilities, storage requirements and costs.

6 Compliance with legal Requirements

6.1 Application of this policy will take account of legal and regulatory requirements as listed below:

Data Protection Act 1998 (DPA)

Protects against the illegal disclosure and misuse of personal data. Any breach of the DPA by an individual leads to personal liability under the act.

Copyright Designs and Patents Act 1988

This includes protection against the unlicensed copying or use of software products.

Computer Misuse Act 2001

The Act identifies three specific offences:

- Unauthorised access to computer material (that is, a program or data);
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime; and
- Unauthorised modification of computer material.

Regulation of Investigatory Powers Act 2000

Creates the offence of intercepting communications on public and private networks unless certain specific conditions are met in which employers may lawfully access employees' communications.

Document Reference	CNC/POL/2.3.5	Page 3 of 4
Uncontrolled when printed unless subject to controlled issue. Refer to Index of Policies for current version		
Policy produced from Template:	CNC/CD/0428 CNPA Policy Template	R 5.0

NOT PROTECTIVELY MARKED

Police and Criminal Evidence Act 1984

Defines conditions under which law enforcement may obtain and use evidence.

Anti-Terrorism, Crime and Security Act 2001, Sect 79

Outlines the criminal offence of disclosing information that could prejudice nuclear security. The provisions are intended to deter anyone contemplating making such disclosures and allow those doing so to be prosecuted.

Human Rights Act 1998

The purpose of providing policy is to give an indication to staff of the expected course of action. However, it is not possible to cater for every possible combination of factors that would justify a departure from the stated policy. The Human Rights Act 1998 requires the proper use of discretion at all times and nothing within this policy and associated procedural instructions prohibits the use of discretion in appropriate circumstances. Where action is taken that has the potential to interfere with an individuals human rights, the reasons behind the making of the decision should be recorded. Such actions should be necessary, reasonable and justified in the circumstances.

Freedom of Information Act 2000.

Exemptions do not apply to this statement of agreed policy under the Freedom of Information Act 2000.

This policy is further and more specifically implemented by the following documents:

Document Reference;

HMG Security Policy Framework

Information Governance Policy: CNC/POL/5.4

Information Security Policy: CNC/POL/2.3.4

ACPO Good Practice Guide for Computer Based Electronic Evidence.

Police & Conduct Regulations 2008: Police Officers

Disciplinary Procedure: Police Staff: CNC/PP/0413

Misconduct Procedure: Police Officer: CNC/PP/0027

Document Reference	CNC/POL/2.3.5	Page 4 of 4
Uncontrolled when printed unless subject to controlled issue. Refer to Index of Policies for current version		
Policy produced from Template:	CNC/CD/0428 CNPA Policy Template	R 5.0