

# GWENT POLICE INFORMATION SECURITY POLICY



Heddlu  
Gwent  
Police

## SUMMARY

The aim of this Policy is to set basic standards to maintain the confidentiality, integrity and availability of all information and information processes throughout the Force. It is the source document for a range of security-related material and will be accompanied by procedural documents and guidance that explain exactly what is required for security compliance in a variety of practices throughout the organisation.

The [Information Security Officer](#) (ISO) is the focal point in Gwent Police for all matters relating to Information Security. The ISO provides advice on information security matters to ensure the implementation of local and national standards through the force Information Assurance Board.

Information Assurance (IA) is about demonstrating that Gwent Police manages information in a consistent, secure manner; ensuring that information is processed legitimately. Appropriate measures are necessary to protect information and assets e.g. documents, people, equipment etc.

Support in understanding what you should do is provided in the [Essential Security Guide](#) which is a brief overview of important security matters which you should find informative and useful in performing your role.

Further detailed Procedures and Work Instructions, developed within the overarching framework of the Information Security Procedure, are provided in the [Information Security Manual](#). This Manual is a dynamic document and subject to change as new threats, and vulnerabilities arise, and countermeasures are introduced. A list of the areas covered can be found under [Information Assurance](#) on the Force Intranet.

**PRINTED VERSIONS SHOULD NOT RELIED UPON. THE MOST UP TO DATE VERSION CAN BE FOUND ON THE INTRANET POLICIES SITE.**

# INDEX

## **1.0 Policy Identification Page**

## **2.0 Policy Statement & Intentions**

- 2.1 Principle & Scope of Policy
- 2.2 Aims of Policy

## **3.0 Introduction**

- 3.1 Origins / Background Information
- 3.2 Motivators / Driving Forces
- 3.3 The Legal Basis and Legitimate Aims

## **4.0 Implications of the Policy**

- 4.1 Financial Implications / Best Value
- 4.2 Human Resources / Training
- 4.3 Strategic Plan Links
- 4.4 Partnership Links
- 4.5 Diversity
- 4.6 Links to Other Policies / Procedures
- 4.7 Consultation

## **5.0 Human Rights Consideration Certification**

- 5.1 Auditing for Potential Interference and Discrimination
- 5.2 Key Human Rights Principles
- 5.3 Rights, Publication, Audit and Inspection
- 5.4 Certificate of Compliance
- 5.5 Legal Vetting

## **6.0 Promotion and Distribution**

## **7.0 Monitoring / Review**

## 1.0 Policy Identification Page

This policy has been drafted in accordance with the principles of Human Rights Legislation. Public disclosure is approved.

### **Policy Title: Information Security Policy**

**Reference:**133/1 a issue 3

### **Reference History:**

Information Security Policy June 2003 issue 2,  
Information Security Policy November 1996 issue 1,  
Previously Data Protection Act 1984 Standing Order 133 dated 8/92.

### **Underlying Procedures:**

Guidance and procedures to support this policy are available on the Force Intranet Information Assurance site under Essential Security Guide and Security Manual.

These will include incident handling, information backup, system access, virus controls, passwords and encryption.

**Policy Ownership:** Information Security Committee  
**Portfolio/Business Area Owner:** ACPO Operation Support  
**Policy Written By:** Information Security Officer  
**Department Responsible:** Standards Department  
**Policy Lead:** Head of Standards Department  
**Links to other Policies:**

- Data Protection Policy
- Freedom of Information Policy

**Policy Implementation Date:** STCG 25<sup>th</sup> April 2006

**Policy Review Date:** March 2008

## **2.0 Policy Statement & Intentions**

### **2.1 Principle & Scope of Policy:**

The objective of this Policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. It enables management to set a clear policy direction in line with the objectives of Gwent Police and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Guidance and procedures produced to support this policy establish and documents an organisational security structure and a clear framework of roles and responsibilities so that all members of the Force are aware of their individual responsibility to safeguard Force information.

This document is endorsed by the Chief Constable as a high-level security statement. The implementation of this policy demonstrates the commitment of the Force in complying with the requirements of the ACPO / ACPO(S) Community Security Policy (CSP) and thus enabling secure information sharing with partner organisations.

### **2.2 Aims of Policy**

The aim of the Information Security Policy is to set basic standards to maintain the confidentiality, integrity and availability of all information and information processes throughout the Force. This will enable the Force to comply with the following:

- i) All legal, statutory and contractual requirements relating to all information and information processes;
- ii) The ACPO CSP and other ACPO guidance relating to information assurance;
- iii) The Manual of Protective Security and its implementation of ISO/IEC 17799 standards (formerly known as BS7799);
- iv) Security education, training and awareness requirements;
- v) Business continuity management;
- vi) Consequences of information security violations.

## 3.0 Introduction

### 3.1 Origins/Background Information

Gwent Police operates through intelligence led policing, it is therefore dependent upon information, and consequently the systems upon which information is processed. This policy sets out the strategic aims and objectives of the Force in relation to information protection for both manual and mechanical systems. Due to the current dependence of almost all organisations upon information communications technology (ICT), as might be expected, the content of this document includes many references to ICT information systems. However, the security of manually held information is equally important and, where appropriate, is covered in some detail in the relevant areas of the policy framework.

The general public has a right to expect that all members of the Force will, when utilising information in connection with Force business, ensure its confidentiality and integrity (particularly in relation to personal information). It is important that the right information is made available to those who need to use it for either operational or administrative purposes. When considering the availability of information employees should understand the benefits of making information available to those who 'need to know' and therefore should follow relevant guidance when supplying information.

The loss, damage, wrongful destruction or wrongful disclosure of information could result in substantial costs to the Force as well as public embarrassment and a reduction in public confidence.

### 3.2 Motivators/Driving Forces

The ACPO Community Security Policy (CSP) is intended to provide a common basis for the 'policing community' to develop, implement and measure effective security management practice and to provide confidence in inter-community dealings and third party access/supply.

### 3.3 The Legal Basis and Legitimate Aims

Gwent Police will comply with the scope of the CSP. This is based on the Manual of Protective Security and its implementation of the International Standard Code of Practice for Information Security Management ISO/IEC 17799 standards (formerly known as BS7799) and covers both technical and non-technical aspects, including:

- Organisational Security Structure;
- Asset Classification and Control;

- Personnel Security (including implementation of the Government Protective Marking Scheme and appropriate employee vetting procedures);
- Physical and Environmental;
- Communications and Operations Management
  - Internal networks
  - External networks (including Internet);
- Internet Access and E-mail Use;
- Access Control;
- Systems Development and Maintenance;
- Business Continuity Management;
- Compliance.

The legitimate aims in accordance with the Human Rights Act 1998 are as follows:

- Necessary in a democratic society;
- In the interests of public safety;
- National security;
- Protection of the rights and freedoms of others.

## **4.0 Implications of the Policy**

### **4.1 Financial Implications/Best Value**

Financial implications will arise from the changes identified as necessary to procedures, equipment, vehicles and accommodation as a result of carrying out Risk Assessments. Divisions and Departments will need to include bids in their budget for funding these changes in order to comply with this policy. Failure to implement changes identified as a result of implementing this policy will result in Gwent Police risking exclusion from partnerships. This policy has been developed from previous versions using Government standards, in consultation with other forces, and as such implementation of this policy is consistent with best value principles.

### **4.2 Human Resources / Training**

Staffing implications will arise from the changes identified as necessary to procedures, equipment, vehicles and accommodation as a result of carrying out Risk Assessments.

There will be training requirements varying from general awareness for all staff, through more role-related training for practitioners and local co-ordinators, to specialist training for experts. Divisions and departments will need to submit bids, where necessary, to the Training Department for inclusion in the Force Training Plan. Failure to implement training identified as a result of implementing this policy will result in Gwent Police risking exclusion from partnerships.

Centrex, who provide central training for the Police Service, are building reference to the Government Protective Marking Scheme into all their courses. Gwent Police Training is also building reference to Information Security and the Government Protective Marking Scheme into all their courses for new entrants.

Use of the Government Protective Marking Scheme within Gwent has been promulgated in General Orders, all Gwent Police staff have been issued with a leaflet explaining the scheme, and Training have copies for new staff.

### **4.3 Strategic Plan Links**

This Policy supports the Force Aim of "Contributing to delivering justice in a way, which secures and maintains public confidence in the rule of law". It does this by providing the framework for maintaining confidentiality, integrity and availability of all information and information processes throughout the Force.

#### **4.4 Partnership Links**

This policy has been developed in order to give Gwent Police the ability to demonstrate to its partners that it is committed to complying with the requirements of the Association of Chief Police Officers Information Systems Community Security Policy (ACPO CSP).

#### **4.5 Diversity**

In the application of this policy consideration must be given to the possible social impact of this policy on the community. A social impact assessment is a requirement to ensure all issues are considered. This is also a requirement of the Gwent Police Race Equality Scheme. Social impact assessments must be undertaken before and after the application of this procedure.

Under the Race Relations (Amendment) Act 2000 Gwent Police is required to undertake proactive work to meet the General Duty of :

- Eliminating unlawful racial discrimination;
- Promoting equality of opportunity;
- Promoting good relations between people of different ethnic groups.

The General Duty is outlined in Section 71 (1) of the Act, and must be met **in its entirety**.

Monitoring must be undertaken to ensure that there is no adverse impact either positive or negative upon any one particular social group or individual. The results of monitoring must be analysed and be available for publication, and Appropriate changes made.

All individuals using this policy must be aware of the potential impact that this policy has on the individuals to whom it is applied. The following strands of diversity and their corresponding pieces of legislation must be considered when answering these questions.

- Welsh Language Act 1993
- Race – Race Relations Act 1976
- Race Relations Amendment Act 2000
- Disability - Disability Discrimination Act 1995
- Gender – Sexual Discrimination and Equal Pay Act 1971
- Age – Article 13 Treaty of Amsterdam (2006)
- Sexual Orientation – Article 13 Treaty of Amsterdam (2003)
- Religion – Article 13 Treaty of Amsterdam (2004)
- Employment Equality (Sexual Orientation) Regulations 2003
- Employment Equality (Religion or Belief) Regulations 2003

#### **4.6 Links to Other Policies / Procedures**

- **Data Protection Policy**

Gwent Police is committed to maintaining the integrity of personal data held on local and national police computer systems as governed by the Data Protection Act 1998, various other Acts of Parliament and ACPO guidance.

- **Freedom of Information**

Gwent Police is committed to complying with the Freedom of Information Act 2000 and procedures have been developed to support that commitment.

- **Vetting Policy**

Through applying National Security Vetting criteria Gwent Police demonstrates commitment to maintaining an acceptable level of assurance as to the integrity of individuals who have access to protectively marked government assets and/or who require access to Gwent Police persons, sites and materials. Force vetting provides a similar level of assurance as to the integrity of individuals who have access to sensitive criminal intelligence, financial, or operational police assets.

#### **4.7 Consultation**

Gwent Police has had an Information Security Policy (Ref 133/1) since 1996. The Policy was revised in 2000 and again in 2002 under the approved revision procedure. In addition to consultations under the relevant revision procedures this latest revision (2003) has, like previous versions, been endorsed by the Force Information Security Committee.

## 5.0 Human Rights Consideration Certification

### 5.1 Auditing for potential interference and discrimination

Q1. What articles of the Human Rights Act 1998 may be engaged?

Article 1  
Article 3  
Article 8  
Article 9  
Article 10  
Article 11  
Article 14

Q2. Where individual rights are engaged what is the potential to discriminate against the parties involved?

Enquiries may be intrusive and there is always the potential to discriminate but this policy will be implemented in a proportionate manner with the intention of ensuring that individuals rights are not unlawfully infringed:

" In the application of this policy the Force will not discriminate against any persons regardless of sex, race, colour, language, religion, political or other opinion, national or social origin, association with national minority, property, birth or other status as defined under article 14 of the European Convention on Human Rights ".

### 5.2 Key Human Rights Principles

Q1. What is the legal basis for your policy?

The application of this Policy is required by legislation including:

- Data Protection Act 1998
- Human Rights Act 1998
- Official Secrets Act 1989
- Copyright Designs & Patents Act 1988
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Interception of Communications Act 1985
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Wireless Telegraphy Act 1949

Q2. Does the policy provide details of what could be considered as a legitimate aim for the potential interference with an individual's rights, through the exercising of this policy? Restrictions on the rights protected in articles 8 - 11 in

the Human Rights Act will be compatible with the convention only if they are aimed at protecting one of the interests listed in articles 8(2), 9(2), 10(2) and 11(2) respectively. The interest protected are broadly the same and generally include:

1. National Security
2. Public Safety
3. The protection of health or morals
4. The prevention of disorder or crime; and the protection of the rights of others.

### **5.3 Rights, Publication, Audit and Inspection**

Q1. What rights to make representation and appeal process are available?

Anyone who feels that a member of Gwent Police staff has behaved incorrectly or unfairly has the right to make a complaint. Initial action should be taken in one of the following ways:

- Complaint to the Standards Department
- Complaint in writing or in person to the Senior Officer at the appropriate police station or in writing to the Chief Constable of the force concerned.
- Visit a local Citizens' Advice Bureau.
- Contact a solicitor.
- Appeal to IPCC

Persons who wish to make representations regarding the operation of this policy should contact the Detective Superintendent Standards.

Gwent Police staff who feel they have grounds for concern in relation to the implementation of this policy may:

- Pursue concerns through their line manager.
- Pursue a grievance formally through the Fairness At Work Procedure
- Seek advice from their staff association or trades union.

Q2. Apart from the Gwent Police Publication Scheme how is the policy made available to the public?

The policy is disclosable to the public. Where copies of this policy are requested they can be made available from the Standards Department.

Q3. What internal review and audit process is in place or is proposed?

This policy has been drafted in accordance with the principles and rights contained within the Human Rights Act 1998. It will be reviewed and continuously assessed in the light of any relevant changes and developments in the application of the Act.

Q4. What external independent scrutiny is recommended?

Independent scrutiny can be where required conducted by the Police Authority and Her Majesty's Inspector of Constabulary.

#### **5.4 Certification of Compliance**

Consideration has been given to the compatibility of this policy with the Human Rights Act by the policy officer; with particular reference to the legal basis of its precepts: the legitimacy of its aims; the justification and proportionality of the actions intended by it; that it is the least intrusive and damaging option necessary to achieve the aims; and that it defines the need to document the relevant decision making process's and outcomes of actions.

#### **5.5 Legal Vetting**

**There are no issues in this policy under ECHR, which cannot be resolved. This policy has been vetted.**

## **6.0 Promotion and Distribution**

This policy will initially be promoted internally, to all staff, through General Orders and the Force Intranet to achieve understanding, awareness, involvement, support and commitment.

Additionally Divisional Commanders / Departmental Heads will have the opportunity to have Information Security as an agenda item at Divisional / Departmental meetings.

Individuals and groups will be encouraged to be involved in the awareness activities and to have responsibility for promotion, implementation and distribution.

The promotional strategies include posters, Internet site, and competitions.

## **7.0 Monitoring / Review**

Monitoring will be in line with the principles of the Race Relations (Amendment) Act 2000.

The application of this Policy will be monitored by the Information Security Board which will deal with the inputs and outputs to the Management Review of Information Security. An example will be through the notification and investigation of security incidents addressing potential breaches and taking appropriate action taken to reduce their occurrence.

Where any person feels that their rights may have been breached as a result of the application or non-application of this policy, they may seek redress through the Grievance Procedure of the Equal Opportunities Policy and Strategy.