

RESTRICTED



**HEDDLU
DYFED-POWYS
POLICE**

Internet Investigations

FORCE POLICY

Author:	Karen Burch
Quality Assurance:	T/DI Shirley Davies
Version:	0.02
Date:	October 2008
Person Responsible:	Det. Chief Superintendent Mears

POLICY IDENTIFICATION PAGE

THIS POLICY HAS BEEN DRAFTED IN ACCORDANCE WITH THE PRINCIPLES OF HUMAN RIGHTS Act 1998. PUBLIC DISCLOSURE IS APPROVED UNLESS WHERE OTHERWISE INDICATED AND JUSTIFIED

POLICY TITLE: Internet Investigations - Force Policy

POLICY REF. NO: 02/09

POLICY OWNERSHIP: Dyfed-Powys Police

PORTFOLIO/BUSINESS AREA OWNERSHIP: CM&RD

DEPARTMENT RESPONSIBLE: CM&RD

PERSON RESPONSIBLE: Detective Chief Superintendent

LINKS/OVERLAPS WITH OTHER POLICIES:

POLICY IMPLEMENTATION DATE: June, 2009

REQUIRED FREQUENCY OF REVIEW: Annually

DATE POLICY LAST REVIEWED: N/A

POLICY REVIEW DATE: February 2010

CERTIFICATE OF COMPLIANCE

This policy has been drafted in accordance with the Human Rights Act 1998 and has been reviewed on the basis of its contents and the supporting evidence and it is deemed compliant with that Act and the principles underpinning it.

Name: Samantha Gainard

Department: Legal Services Department

Signed:*S. Gainard*..... (Force Legal Advisor)

REVIEW

This policy is due for review by:*February, 2010*.....

Review of Document

Date of Review	Reviewed by:	Amendments made

Contents

<i>Section</i>		<i>Page</i>
	General Principles	5
	Aim and Lawful Authority	5
1.	Introduction	6
2.	Role of Network Investigator (Section 31(1) (a)(b)(c) Law Enforcement exemption applied to some information)	6
3.	(Section 31(1) (a)(b)(c) Law Enforcement exemption applied)	8
4.	(Section 31(1) (a)(b)(c) Law Enforcement exemption applied)	11
5.	(Section 31(1) (a)(b)(c) Law Enforcement exemption applied)	11
6.	(Section 31(1) (a)(b)(c) Law Enforcement exemption applied)	11

Policy Document Statement

This Policy has been drafted in accordance with the Human Rights Act 1998.

General Principles

It is the policy of Dyfed-Powys Police:

- To deliver guidance in respect of internet investigations.
- To clearly define administrative duties in support of key policing objectives.
- To provide key information to front line officers.
- To work in partnership with other agencies to protect the public and prevent crime.

All staff in the adoption of this policy and in the exercise of their daily duties must ensure that:

- a. They follow a clearly defined decision making process by detailing their objective(s), assessing all available and relevant information and feasible options, documenting decisions, and reviewing outcomes;
- b. They give due regard to the welfare, safety, general well being and human rights of all individuals;
- c. They do not unjustifiably discriminate against any individual or groups of individuals;
- d. Actions taken are justified, strictly proportional to, and the least intrusive and damaging option to the achievement of their legitimate aims;

Aim and Lawful Authority

The purpose of this policy is to provide guidance to police personnel relating to the investigation of internet facilitated crime.

The legal basis for the exercise of powers and duties outlined in this policy are:

- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Police and Criminal Evidence Act 1984

Dyfed-Powys Police consider that these actions are necessary in a democratic society in the interest of, and in order to safeguard:

- Public safety
- The prevention of disorder or crime
- The protection of public order
- The protection of rights and freedoms of others

1. INTRODUCTION

In recent years the volume of internet crime reported and recorded in relation to computer issues has increased considerably within the force.

Internet crime affects both the public and private sector, with viruses and other malicious programs controlling computers around the world for criminal purposes.

The internet is also increasingly being used by all ages for social networking, communication, transferring of funds and purchasing goods and services. The perception by many users is that the internet gives anonymity and protects privacy.

This is not necessarily the case and as a result it has become a vehicle for criminals to facilitate crime such as fraud, paedophilia and harassment.

Users are becoming increasingly willing to provide personal information whether it is available to other users or just the company running the service.

Due to the publicly displayed personal information regarding lifestyle, acquaintances, personal photographs and online diaries containing opinion, the internet has also become an excellent source of intelligence and information, both for legal and illegal use and once made public, information on the internet in many cases cannot be deleted.

The aim of this document is to provide guidance to Officers within force on how to deal with crime that involves the use of the internet and how the Force Network Investigator can assist and is integral to that process.

2. ROLE OF THE NETWORK INVESTIGATOR

The Network Investigator is situated within the Crime Management and Reduction Department and is based within the Force Intelligence Bureau (F.I.B) at Headquarters. The post holder is under the line management of the Detective Inspector F.I.B.

(Section 31(1) (a)(b)(c) Law Enforcement exemption applied)

3. (Section 31(1) (a)(b)(c) Law Enforcement exemption applied)

4. (Section 31(1) (a)(b)(c) Law Enforcement exemption applied)

5. (Section 31(1) (a)(b)(c) Law Enforcement exemption applied)

Internet safety advice is also available to members of the public can be found on the external Dyfed Powys Police website;

<http://www.dyfed-powys.police.uk/en/advice/internet/new.htm>

6. (Section 31(1) (a)(b)(c) Law Enforcement exemption applied)