

Dyfed Powys Police

Data Protection Policy
HQ Policy Ref No: 12/01

Author	Claire John	Dept	Data Protection Professional Standards
Version	5	Date	31 January 2001
Human Rights Act Certification	Mr M Beckett (Force Legal Advisor)	Date	12 February 2001
Approved By	HRSG	Date	6 March 2001
Ratified By	ACC	Date	6 March 2001
Review Date	September, 2009		

Document History

Version	Date	Author	Reason for Change
2.0	14.01.2005	John Evans	REVIEW
3.0	27.04.2006	John Evans	REVIEW
4.0	May 2007	John Evans	Review and update Separate policy from procedure
5.0	June 2008	John Evans	Review and update Inc. MOPI

Consultation Circulation List

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 content and the supporting evidence and it is deemed compliant with that Act and the principles underpinning it

Name: Bryn Thomas

Department: Legal Services

Signed: *B Thomas*

Policy Contents

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

1. Policy

- 1.1 Dyfed Powys Police processes personal data and has a duty to notify (register) with the Information Commissioner. The Registration Number Z489524X is recorded in the Information Commissioner Register of data controllers.
- 1.2 The Chief Constable is the Data Controller for Dyfed Powys Police (DPP). Management of the statutory obligations and the force data protection policy is delegated to the Force Data Protection Officer.
- 1.3 The overarching purpose for which the Police are registered with the Information Commissioner is the prevention, detection of crime, apprehension, prosecution of offenders, maintenance of law and order, protection of life and property, vetting and licensing, public safety and rendering assistance to members of the public in accordance with force policy.
- 1.4 In addition to the 'policing' purpose Dyfed Powys Police are also registered for the support purposes of (1) staff administration which covers appointments or removals, pay, discipline, superannuation, work management or other personnel matters in relation to staff and (2) administration and ancillary support for policing purpose which includes records of computer transactions/computer message logs, telephone message logs, police property management logs etc.
- 1.5 Dyfed Powys Police has a legal obligation to comply with the Data Protection Act 1998, the Computer Misuse Act 1990, the Freedom of Information Act 2000, the Copyrights, Designs and Patents Act 1998 and the Human Rights Act 1998. As well as ensuring compliance with the ACPO Manual for Data Protection Management, ACOPO Community Security Policy and the Police National Computer System Security Policy and the Guidelines for the Management of Police information.
- 1.6 Exchange of information is an essential ingredient in our quest to achieve our objectives. We will therefore, where appropriate and in line with legislation, disclose or exchange personal information with other agencies, organisations or persons.
- 1.7 In the exercise of any power, authority or directive under this policy, each member of staff must:
 - a) give due regards to the privacy and human rights of all individuals
 - b) make full use of all current and relevant legislation

c) not unjustifiably discriminate against any individual or group of individuals

d) ensure that each action taken is justified and strictly proportionate to and is the least intrusive and damaging option required to secure the achievement of the legitimate aims

- 1.8 That in the carrying out of this duty, it will be the duty of staff to follow a clearly defined decision making process by detailing their objectives, assessing all available and relevant information and options, documenting decisions made and reviewing outcomes.
- 1.9 This decision making process will be the subject of review and scrutiny by supervisors, managers and other parties as appropriate.
- 1.10 This policy is aimed at every member of Dyfed Powys personnel whether employed, contracted or a volunteer including those external to Dyfed Powys Police who have access to our information/systems and the communities of Dyfed Powys Police.

2. Aim and Lawful Authority

- 2.1 In order to achieve the lawful handling of personal data, the aim of Dyfed Powys Police will be to comply with the eight Data Protection principles:
- data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
 - data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes
 - data shall be adequate, relevant and not excessive in relation to the purpose of purposes for which they are processed
 - data shall be accurate and, where necessary, kept up to date
 - data shall not be kept for longer than necessary for that purpose or those purposes
 - data shall be processed in accordance with the rights of data subjects under the act
 - **AND THAT**
 - appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of , or damage to personal data
 - data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data
- 2.2 Dyfed Powys Police needs to collect and use certain types of information about the people with whom it deals in order to perform effectively as a police force. These include current, past and prospective members of staff, offenders, victims, witnesses, suppliers,

clients/customers and others with whom it communicates. This personal information must be dealt with properly when it is collected, recorded, used and destroyed, whether by manual or electronic means. DPP regard the lawful and correct treatment of personal information as important to the successful operation of the Force, achievement of our aims and objectives and to maintaining the confidence of members of the public. Numerous recording systems exist within the organisation and the integrity and value of this information is paramount. The communities served by Dyfed Powys Police expect data to be treated in line with legislation. If any breaches of the Data Protection Act 1998 do take place then these will be dealt with in accordance with this policy.

2.3 Dyfed Powys Police will ensure access is provided for individuals who are lawfully entitled to such information in accordance with Section 7 of the Data Protection Act 1998.

2.4 The legal basis for the exercise of any power, authority or directive under this policy is:

- Data Protection Act, 1998
- Crime & Disorder Act 1998
- Police Act 1996
- Police Act 1997
- Police and Criminal Evidence Act 1984
- Rehabilitation of Offenders Act 1974
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Code of Practice on the Management of Police Information 2005
- ACPO Data Protection Manual of Guidance
- PNC National Operating Rules
- Dyfed Powys Information Security Policy and Information Technology Strategy
- The National Strategy for Police Information Systems including the Police Community Security Policy

2.5 Dyfed Powys Police consider that any action taken under this policy is necessary in a democratic society in the interests of:

- National security
- Public safety
- Economic well-being of the country
- Prevention of crime and disorder
- Protection of health and morals
- Preventing the disclosure of information received in confidence
- Protection of the reputations, rights and freedom of others

3. Definition of Terms

- 3.1 Data Controller – means a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed.
- 3.2 Personal Data – means data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.

It includes expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.0 CONSEQUENCES OF NON COMPLIANCE

- 4.1 The Data Protection Act 1998 grants extensive power to the Information Commissioner and provides more extensive rights for the individual. An individual has the right to claim compensation for damage or distress suffered as a result of non-compliance, be it inappropriate processing or poor data quality. If an individual complains to the Office of the Information Commissioner then the Information Commissioner is obliged to investigate to establish if a breach of the Data Protection Act 1998 has occurred.

4.2 Enforcement

- 4.3 The Commissioner can serve a Data Controller with an 'information notice' requiring the Data Controller to provide certain information within set time limits. Failure to comply with such a notice, or providing deliberately false information, is a criminal offence.
- 4.4 If the Commissioner concludes that there has been a breach of the Act, he may then serve a Data Controller with an 'enforcement notice'. This could force a Data Controller to cease processing personal data, or cease processing data in a particular way which could be catastrophic for the Force. Failure to comply with an enforcement notice is a criminal offence.

5.0 CRIMINAL OFFENCES

- 5.1 A number of criminal offences are created by the Data Protection Act. The data controller is guilty of an offence if they
- (a) are processing without notification;
 - (b) fail to notify the Commissioner of changes to notification register entry;
 - (c) fail to comply with written request for particulars;
 - (d) fail to comply with an enforcement notice/information notice/special

information notice;

(e) knowingly or recklessly make a false statement in compliance with an enforcement notice or special information notice;

(f) intentionally obstructs, or fails to give reasonable assistance in the execution of a warrant.

5.2 However, it is not just the Data Controller who is criminally liable. Police Officers and Police Staff in Dyfed Powys Police are considered to be servants or agents of the Chief Constable (the Data Controller) and as such can be personally criminally liable if they disclose or obtain personal data without the authority of the Data Controller. Therefore, if you make, or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable. The offences that apply are given at Section 55 of the Act and are as follows:

- (a) without the consent of the Chief Constable (Data Controller), knowingly or recklessly to unlawfully obtain or disclose personal data or the information contained in personal data; or procure the disclosure to another person of the information contained in personal data;
- (b) without the consent of the Chief Constable (Data Controller) to knowingly or recklessly procure the disclosure to another person of the information contained in personal data.
- (c) There is another offence committed by a person who sells personal data if it has been obtained in contravention of the above or offers to sell information obtained or to be obtained in contravention of the above.

This does not apply if it can be shown: -

(i) that the obtaining, disclosing or procuring -

- was necessary for the purpose of preventing or detecting crime,

or

- was required or authorised by or under any enactment, by any rule of law or by the order of a court,

(ii) that an individual acted in the reasonable belief that they had in law the right to obtain or disclose the data or to procure the disclosure to another person,

(iii) that they acted in the reasonable belief that the Chief Constable would have consented if they had known of the obtaining, disclosing or procuring and the circumstances of it, or

(iv) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

In addition, in respect of computer processed information, the following activities are criminal offences under the Computer Misuse Act 1990:

- . unauthorised access to computer material;

- . unauthorised modification of computer material, and

- . unauthorised access with intent to commit/facilitate the commission of further offences.

6. SUBJECT ACCESS

6.1 The Data Protection Act 1998 provides that subject to certain provisions, an individual shall be entitled:-

- (a) to be informed by the Data Controller whether data held includes personal data of which that individual is the subject; and
- (b) to be supplied by the Data Controller with a copy of the information constituting any such personal data held by him.

6.2 A time limit of forty days is specified by the Act, to reply to such requests. The Force will comply with the requirements of the Data Protection Act 1998, in respect of Subject Access to information held by DPP. Subject Access requests will only be processed through the Data Protection Unit.

7. Derogations

Nil

8. Enforcement and Reporting

8.1 All staff, in particular managers and supervisors, will be responsible for the implementation and operation of this policy.

9. Accessibility, Redress and Reviews

9.1 This policy will be published and made readily available to all police officers and police staff via the Force Intranet System.

9.2 This policy is a public document and will be made available to the general public via the Force Publication Scheme – www.dyfed-powys.police.uk - and upon written request to the Force policy coordinator.

9.3 This policy will be reviewed annually by the Head of Data Protection and verified by Legal Services to ensure compliance with Human Rights, other legislation and guidance documents.

There will also be subject to audit by Her Majesty's Inspector of Constabularies (HMIC). The policy will be published in a format making it easily readable.

9.4 Any person(s) who has / have cause to feel aggrieved by any matter outlined in this policy is / are able to and may seek redress in the following ways;

- Misconduct procedures
- Civil or criminal proceedings
- Direction and control procedure
- Reconciliation procedure

- 9.5 Any person in exercising their right, as detailed in paragraph 6.4 above, will have the right of equal access to information and the right to seek legal advice.
- 9.6 Public consultation is an important part of this process, with views and comments welcomed. These should be addressed to the

Chief Constable,
Dyfed-Powys Police Service,
P.O. Box 99,
Llangunnor,
Carmarthenshire.
SA31 2PF.

NOT PROTECTIVELY MARKED

NOT PROTECTIVELY MARKED