

PRACTICE DIRECTION

Title: Data Protection	URN CDB 3039
-------------------------------	---------------------

1. INTRODUCTION

- 1.1 The purpose of this practice direction is to ensure that all personal data is processed in accordance with the principles of the Data Protection Act 1998 (The Act).

2 AUTHORITY LEVELS

- 2.1 The Data Protection Officer is responsible for the management of this Practice Direction.
- 2.2 Amendments to this document that may affect a strategy or may be regarded as contentious, will be referred to Chief Officer Group for approval.

3 ROLES & RESPONSIBILITIES

- 3.1 The Act creates a number of important roles as follows:

Data Controller - The Chief Constable is the Data Controller for ALL Personal Data processed by Humberside Police.

Data Protection Officer – The DPO is responsible for all Data Protection matters pertaining to Humberside Police and manages the Chief Constables statutory obligations under the Act.

- 3.2 All staff employees and in particular line managers and supervisors have responsibility to ensure that this policy is adhered to.
- 3.3 Induction training will be provided on Data Protection by 'Learning and Development Unit and or Data Protection staff.
- 3.4 All staff are encouraged to maintain an awareness through the Computer Based Training package available on the Information Compliance website.

4 AIM AND LAWFUL AUTHORITY

- 4.1 The Data Protection Act 1998 applies to the processing of Personal Data contained within any I.T. system and most paper based systems. Exceptions to paper based systems where the system is unstructured.

In order to achieve lawful handling of personal data, Humberside Police must comply with the Eight Data Protection Principles:

- **Personal data must be processed fairly and lawfully.**

Fairly - Individuals must not be misled as to what their information is to be used for

Lawfully – Adherence to the common law duty of Confidentiality and other statute.

- **Personal data must be obtained only for specified and lawful purposes.**

Data must not be collected unless there is a specified and valid reason.

Any Personal data processed by Humberside Police must only be used for a Policing Purpose, That is:

Protecting of life and property

Preserving Order

Preventing the commission of offences

Bringing offenders to justice,

And any duty or responsibility of the police arising from common or statute law.

- **Personal data must be adequate, relevant and not excessive in relation to the purpose for which held.**
- **Personal data must be accurate and kept up to date.**
- **Personal data should not be held longer than is necessary for the purpose.**

For more detail about the Principles 3, 4 & 5 see our Force Records Management Policy

http://intranet.humberside.police.uk/Branches/Corporate_Development/Information_Compliance/Records%20Management%20Section/RMSLibrary.htm

- **Personal data must be processed in line with data subject's rights.**

The right of subject access entitles individuals to a copy of any information held on them.

Data subjects have the right to prevent processing which may cause damage or distress, they can also claim compensation for any damage caused.

- **Personal data should be surrounded by appropriate security against unauthorised processing, accidental loss, damage or destruction.**
- http://intranet.humberside.police.uk/Branches/Corporate_Development/Information_Compliance/Information%20Security%20Section/InformationSecurityDocumentation.htmstruction
- **Personal data must not be transferred overseas.** Data shall not be transferred to a country of territory outside the EEA unless that country as an adequate level of protection.)

Staff should liaise with ICU where such transfers are necessary, to ensure appropriate security is applied.

5. FAIR PROCESSING

- 5.1 Humberside Police collects and uses certain types of information about the people with whom it deals in order to perform effectively as a police force. This includes current, past and prospective members of staff, offenders, victims, witnesses, suppliers and others with whom it communicates. This personal information must be dealt with properly when it is collected recorded used and destroyed.
- 5.2 Humberside Police regard the lawful and correct treatment of personal information as vitally important to the successful operation of the Force and to maintaining public confidence.

6. POLICING PURPOSE

- 6.1 The overarching policing purpose for processing personal data of which the Police have 'notified' the Information Commissioner includes.... the prevention, detection of crime, apprehension, prosecution of offenders, maintenance of law and order, protection of life and property, public safety and rendering of assistance to members of the public in accordance with force policy,
- 6.2 In addition to the 'policing purpose' Humberside Police are also registered for support purposes of staff administration covering pay, discipline, appointments or any other personnel matters and administration and ancillary support for policing purpose.
- 6.3 The Data Protection Officer is available to give specialist advice regarding the possible contravention of DP legislation and should be consulted at an early stage in any suspected or alleged malpractice.

7. CONSEQUENCES OF NON COMPLIANCE

The Information Commissioner is the body that oversees compliance with the Data Protection Act and has powers to force organisations to process personal data lawfully. If an individual complains to the Information Commissioner Office (ICO) then the ICO is obliged to investigate to establish if a breach under the Act has occurred.

The ICO can serve the Data Controller with an 'information notice' requiring the Data Controller to provide certain information within set time limits or an 'enforcement notice' which could force the Data Controller to cease processing personal data in a particular way which could have serious implications for Force. Failure to comply with either is a Criminal Offence.

A number of Criminal Offences are created by the Act, however it is not just the Data Controller who is criminally liable. Police Officers and Police Staff are considered to be agents of the Chief Constable 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 you may be held criminally liable.

The offences under s55 of the Act are knowingly or recklessly unlawfully obtain or disclose personal data, procuring the disclosure to another person or selling personal data.

Individuals also have a right of access to personal data held about them managed by the ICU (see Subject Access PD). They also have the right to claim compensation for damage or distress suffered as a result of non compliance

8 OTHER REFERENCES

Data Protection Act 1998
Human Rights Act 1998
ACPO Data Protection Manual of Guidance
Race Relations Act 1976
Subject Access Practice Direction
Information Security Policy
Records Management Policy

ADMIN

Practice Direction Version	1.0
----------------------------	-----

Owner	Branch	Role
Mrs Clement	CDB	Senior Information Compliance Officer

	Signature	Date
Risk Assessment	S Page	21/09/2011
Equality Impact Assessment	S Page	21/09/2011
Human Rights Impact Assessment	S Page	21/09/2011

	Date Done	Next Date
Publication	21/09/2011	
Review		