#

# Data Protection

# (Policy & Procedure)

**NOT PROTECTIVELY MARKED**

|  |  |
| --- | --- |
| Publication Scheme Y/N | Can be published on Force Website  |
| Department of Origin | Professional Standards Department (PSD)  |
| Policy Holder | Ch Supt Head of PSD |
| Author | Information Governance Manager |
| Related Information | ACPO Data Protection Manual[Authorised Professional Practice: Decision](http://www.ncalt.pnn.police.uk/app/Final%20PDFs/APP_DecisionMaking.pdf)[Making](http://www.ncalt.pnn.police.uk/app/Final%20PDFs/APP_DecisionMaking.pdf) [Data Protection Act 1998](http://www.legislation.gov.uk/ukpga/1998/29/contents)[Regulation of Investigatory Powers Act](http://www.legislation.gov.uk/ukpga/2000/23/contents)[The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000](http://www.legislation.gov.uk/uksi/2000/2699/contents/made)DP/IS Awareness Booklet |
| Date First Approved at BMG | 25/1/2012 |
| This Version | Version 1.0 - Created 26/1/2012 |
| Date of Next Review | 26/1/2016 |

# MP_tagline_colour_a4 January 2012

**Policy**

**Statement**

Merseyside Police is committed to ensuring that all its officers, staff and agents undertake their legitimate duties in a manner compatible with data protection principles set out in the Data Protection Act 1998 (herein after described throughout this policy as ‘the Act’).

The Act regulates the use of information from which a living individual can be identified. It applies to the processing of personal data in most formats including electronic, paper and other media.

**Aims**

The main aim of this policy is to ensure that Force-owned personal information is used appropriately in compliance with the requirements of the Act and that all officers and staff are clear about what is regarded as acceptable or improper use.

The policy is underpinned by procedure that sets out minimum standards and details how those employees and any other authorised person having access to any force systems may use Force-owned personal information lawfully.

##### Objectives

A broad objective is to protect individuals from the use of inaccurate personal information, or misuse of accurate personal information. More specific associated objectives are to:

1. Ensure all persons having access understand their responsibilities regarding their use of personal information
2. Eradicate unlawful use of personal information
3. Safeguard all personal information
4. Protect the reputation of Merseyside Police by strict compliance with the Act and MOPI guidance.

##### Application and Scope

All police officers and police staff, including the extended police family and those working voluntarily or under contract to Merseyside Police who have access to personal information must be aware of, and are required to comply with, all relevant policy and associated procedures.

This policy applies to persons at all levels of the organisation including all Police Officers, Police Staff, Special Constabulary, PCSOs, temporary staff, partner agency staff, consultants, contractors and volunteers.

Merseyside Police will take criminal and/or disciplinary action against any category of person mentioned above who wilfully accesses and/or misuses personal information held by Merseyside Police.

Any use of personal information that does not have a clear policing or other statutory or business purpose is likely to constitute a misuse. Using information is described as “processing” in the Act. See Part 1 1(1) of the Act that describes the ways in which data is defined as having been processed (used).

Section 55 of the Act identifies the following criminal offence:

A person must not knowingly or recklessly, without the consent of the Chief Constable

1. obtain or disclose personal data or the information contained in the personal data, or
2. procure the disclosure to another person of the information contained in personal data.

The Chief Officer lead for this policy is the Deputy Chief Constable.

**Outcome Evaluation**

The Anti-Corruption Unit will retain responsibility for monitoring the use of personal information. Relevant data will include number of cases of misuse of personal information investigated by the ACU and complaints/referrals to PSED on associated issues.

**Contents**

[Usage](#one)

 [Definitions](#oneone)

 [Purpose](#onetwo)

[Processing](#two)

[Lawful](#twoone)

[Fair](#twotwo)

[Notification](#twothree)

[Exceptional Case Review](#twofour)

[Disclosure](#three)

[Personal Data](#threeone)

[Live Data](#threetwo)

[Other Organisations](#threethree)

[Section 29(3) Exemption](#threefour)

[Subject Access](#threefive)

[FOI](#threesix)

[Data Integrity](#four)

[Adequacy & Relevance](#fourone)

[Accuracy](#fourtwo)

[Review, Retention & Disposal](#fourthree)

[Information Security](#fourfour)

[Audit & Monitoring](#five)

[Police Systems](#six)

[Design & Development](#sixone)

[Operating Rules & Conventions](#sixtwo)

[Roles & Responsibilities](#seven)

 [Data Controller](#sevenone)

 [Data Protection Officer](#seventwo)

 [Managers/Supervisors](#seventhree)

 [All Officers, Staff & Contractors](#sevenfour)

 **Procedure**

**1. Usage**

* 1. **Definitions**

1.1.1 Personal data is defined as data that relates to a living individual who can be

identified from that data or, from that data and other information that is, or is likely, to come into the possession of the Data Controller.

* + 1. For the purposes of this document the words ‘data’ and ‘information’ have the same meaning.

1.2 **Purpose**

1.2.1 The Force needs to collect and use certain types of information about people with whom it deals in order to operate. These include victims, current, past and prospective employees, people with criminal convictions, suppliers and others with whom it communicates.

1.2.2 The Force may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments, for example ethnic monitoring of staff, or disclose personal information to comply with other legislation, for example disclosure within Crime and Disorder protocols.

1.2.3 This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material. There are safeguards to ensure this in the [Data Protection Act](http://www.legislation.gov.uk/ukpga/1998/29/contents).

1.2.4 The lawful and correct treatment of personal information is regarded by Merseyside Police as imperative to successful operations, and to maintaining confidence between those with whom we deal and ourselves. The Force needs to ensure that the organisation treats personal information lawfully and correctly.

**2.** **Processing**

2.1**Lawful Processing of Personal Data**

2.1.1 The principal purpose for which Merseyside Police processes information is a ‘Policing Purpose’. This is defined as:

a) Protecting life and property

b) Preserving order

c) Preventing the commission of offences

d) Bringing offenders to justice

e) Any duty or responsibility arising from statute or common law.

Information is also processed for specific purposes connected with the administration of the Force and its employees.

2.1.2 Access to information systems or personal data including browsing, use or disclosure is permitted only to employees, agents and approved persons working for or with the police, where it is necessary in the course of their official duties for policing purposes.

2.1.3 The use of police information systems for a private purpose or any other purpose other than that declared by the Chief Constable to the Information Commissioner is prohibited.

2.1.4 Deliberate unauthorised access to, copying, destruction and/or alteration of, or interference with any computer or ancillary equipment or data (soft or hard copy) is an offence carrying a term of imprisonment under section 1 of the Computer Misuse Act 1990 and therefore strictly prohibited.

* + 1. In order to meet the requirements for lawful processing, particular consideration will be given to:

a) Confidentiality arising from the relationship between the Force and any individual;

b) The ‘ultra vires’ rule and the rule relating to the excess of delegated powers, under which officers may only act within the limits of their legal powers;

c) The legitimate expectations of any individuals in relation to the processing of information about them; and

d) Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence).

2.1.6 Further advice and guidance is available from the Force Information Governance Manager.

2.2 **Fair Processing**

2.2.1 In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as is necessary to ensure that they are likely to understand:

a) The purposes for which their personal data are to be processed;

b) The likely consequences of such processing; and

c) Whether particular disclosures can reasonably be envisaged.

2.2.2 Further advice and guidance is available from the Force Information Governance Manager

2.3 **Notification**

2.3.1 The National body for the supervision of Data Protection is the Information Commissioner to whom the Chief Constable notifies his purposes for processing personal data.

2.3.2 That notification process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the Data Protection Act 1998 that the public should know, or be able to find out, who is carrying out the processing of personal data and for what purpose.

2.3.3 Copies of the Merseyside Police Notification details are available upon request from the Force Information Governance Manager.

2.4 **Exceptional Case Review**

2.4.1 Processing of requests for the deletion of conviction information, fingerprints, DNA and photographs should be carried out in accordance with the advice and guidance provided by the ACPO CRO. This is currently a centralized function within the Corporate Criminal Justice Unit.

**3.** **Disclosure**

3.1 **Personal Data**

3.1.1 Information from police information systems will, in the first instance, only be disclosed to serving officers or other police personnel, who require such information in order to carry out their official duties. The information held is for police use only but may in approved and established circumstances be supplied to other persons or organisations at the discretion of the Chief Constable.

3.1.2 Requests for the disclosure of any personal information will only be considered once the member of staff, is fully satisfied that the enquirer or recipient is authorised to receive the information.

3.1.3 Care must be taken to ensure that any disclosure is within that allowed by any prevailing policy, guidance, Information Sharing Agreement, Memoranda of Understanding or statutory obligation or statutory provision and is authorised at the appropriate level.

3.1.4 Further specific advice and guidance concerning any aspect of information sharing or disclosure may be obtained from the Information Governance Manager or from the Partner Agency Consort Team (PACT)

3.2 **Live Data**

3.2.1 To avoid any unintentional and/or unlawful disclosure, the use of ‘Live’ data held on computer systems or in manual filing systems for training, testing or practice purposes is strictly prohibited without prior and express consultation with the Force Information Governance Manager.

3.3 **Other Organisations**

3.3.1 There are times where it is necessary to seek information relevant to a police enquiry from other organisations (credit details, phone / bank account details etc.).

3.3.2 In these circumstances, the organisation receiving the police request may request an official form stating the reason and what specific information is sought.

* + 1. The exemption to the rules of non-disclosure, which is most likely to affect police officers, provides that personal data is exempt from the non-disclosure provisions of the Act in cases where the disclosure is for any of the following purposes:

(a) The prevention and detection of crime

(b) The apprehension or prosecution of offenders

3.3.4 These exemptions only apply to the extent that if the data were not disclosed to the police it would be likely to prejudice police investigations.

3.3.5 In all circumstances a Section 29(3) exemption Form must be used.

3.3.6 It should be noted that although we are able to use section 29(3) for legitimate police enquiries it is still a matter for the organisation to determine whether or not to disclose information, as there is no element of compulsion in this respect.

3.3.7 A brief pocket notebook entry must also be made of every such transaction. Where pocket notebooks are not used, then an appropriate entry must be made on the source document for each transaction.

3.3.8 If an Information Sharing Agreement (sometimes also known as a Protocol or a Memorandum of Understanding) is in existence the rules of that agreement should be followed.

3.3.9 Where disclosure is in the vital interest of the data subject there are provisions under the Act which cater for circumstances where there is a genuine life or death situation (severe medical emergency or a potential suicide are examples) and where the usual approach of obtaining consent for a disclosure is not possible or has been unreasonably withheld.

3.3.10 These provisions are contained within Schedules 2 & 3 of the Act and refer to the vital Interests of the data subject.

3.3.11 Officers making use of this process should ensure that the events are adequately documented and retained pending any future challenge over possible unlawful processing of personal data.

3.3.12 Further advice and guidance is available from the Force Information Governance Manager

3.4 **Section 29 (3) Exemption**

3.4.1 Other organisations may also request information from the police under the non-disclosure exemption provided by Section 29(3).

3.4.2 Normally such use will be by organisations that have the ability to investigate and/or prosecute offences.

3.4.3 It should be noted that there is no obligation for the Force to comply with

such a request and any disclosure must only be made in accordance with relevant Force policies and/or prevailing legislation.

* + 1. Each request must be considered on its individual circumstances and disclosures made only where the relevant considerations are satisfied. The receipt of such requests together with the decision and any relevant responses should be recorded and retained on the appropriate file and available for any future audit or inspection.

3.4.5 In order to provide appropriate accountability all responses to section 29(3) requests must be countersigned by an officer of at least the rank of Inspector of police staff equivalent.

**3.5 Section 35 Exemption**

* + 1. Other organizations may also request information from the police under section 35 that provides a legal gateway for disclosure should the disclosure of specific information be necessary for the purpose of any legal proceedings or for the purpose of obtaining legal advice.

3.5.2 It should be noted that there is no obligation for the Force to comply with

such a request and any disclosure must only be made in accordance with relevant Force policies and/or prevailing legislation

* + 1. Each request must be considered on its individual circumstances and disclosures made only where the relevant considerations are satisfied. The receipt of such requests together with the decision and any relevant responses should be recorded and retained on the appropriate file and available for any future audit or inspection.
		2. In order to provide appropriate accountability all responses to section 29(3) requests must be countersigned by an officer of at least the rank of Inspector of police staff equivalent.

3.6 **Subject Access**

3.6.1 Section 7 of the Act gives individuals the right of access to personal data held about them through the subject access provisions.

* + 1. For information on the administration and processing of subject access requests see the Subject Access section on the Force Internet site.

3.6.3 Further advice and guidance may be sought from the Force Information Governance Manager

3.7 **Freedom of Information Act 2000 (FOI)**

3.7.1 The FOI Act extended the provisions of the rights given under the Data Protection Act for persons to request information held by public sector organisations.

3.7.2 The effect of those changes is that (subject to certain exemptions) the subject

access and FOI provisions now cover most forms of information held by the Police, including; computer, manual records and other media.

3.7.3 FOI enables any person in the world to request information from any UK Public Sector organisation, whether for personal or non-personal data. When a request is for personal information it must still be dealt with in accordance with the provisions of the Data Protection Act 1998.

3.7.4 See also the Force Freedom of Information Policy. Further advice and guidance is available from the Force Information Governance Manager and the FOI Review Officer, Information Bureau.

**4.** **Data Integrity**

4.1 **Adequacy & Relevance**

4.1.1 The reliability of information held in police information systems depends primarily on the professional competence of police officers and staff who obtain and record information.

4.1.2 Information held on police information systems must be adequate, i.e., fit for purpose, unambiguous and professionally worded. All abbreviations, warning signals and information markers used must comply with national standards.

* + 1. Forms designed for the collection of information should only request that information which is pre-determined to be relevant in relation to the purpose for which it is required. Enquiry or application forms should include a ‘fair processing notice’ where appropriate. The following link provides the Information Commissioner’s guidance on Fair Processing Notices

[ICO Fair Processing Notice Guidance](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_1.aspx). Further information on Fair Processing notices can be obtained from the Information Governance Manager.

4.1.4 Criminal intelligence will be graded using the 5x5x5 evaluation system in accordance with the National Intelligence Model and MOPI standards, which gives an indication of the quality of the information and the reliability of the source.

4.2 **Accuracy**

4.2.1 It is the responsibility of the person who receives the original information to ensure, as far as is possible, that it is accurate, valid, and up-to-date.

4.2.2 All staff should ensure that all information entered on police records is adequate, relevant, unambiguous and professionally worded. Where errors are found on any personal information held they will be reported to a supervisory officer and corrected at the earliest opportunity.

4.2.3 Cancellations, amendments and deletions should be carried out as a matter of priority. However, in order to retain the Force’s corporate memory of our interaction with the person(s) concerned if inaccurate personal information is found and subsequently corrected consideration must be given to retaining the original information, with an appropriate entry being made to direct all future users of that information to the corrected data.

4.2.4 The source of information received from an individual or from a third party must be recorded accurately. Notations of this nature will assist any investigation, should the information or its source be challenged.

4.2.5 Where it is known that inaccurate information may have been disclosed to a third party, the corrected information should be disclosed to that party with explanation, together with any other action necessary to minimize any harm, loss or damage arising from such disclosure.

4.3 **Review, Retention and Disposal of data**

4.3.1 Unless a system incorporates automatic facilities or other structured procedures, reviews of personal data must be carried out at frequent intervals to ensure immediate cancellation or amendment of unneeded or out-of date material. This is good practice that should be applied to all information held for policing purposes.

4.3.2 The Force Records Retention Schedule and other legal requirements for the retention of documents should be referred to for further guidance on this subject.

4.4 **Information Security**

* + 1. Principle 7 of the [Data Protection Act 1998](http://www.legislation.gov.uk/ukpga/1998/29/contents) requires that appropriate technical and organisational measures shall be taken to protect data against:
1. Unauthorised access;
2. Unauthorised or unlawful processing;
3. accidental loss, destruction or damage.

4.4.2 Appropriate technical and organisational security measures include;

a) Using and developing technological solutions to ensure compliance with the data protection principles

b) Using and developing physical measures to protect force assets

c) Ensuring the reliability of any persons who access police information

d) Reporting and investigating security breaches

4.4.3 These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction or damage. The Government Protective Marking Scheme provides for such considerations and is adopted by the Force as part of its compliance with the ACPO Community Security Policy.

4.4.4 All printout material, magnetic tape, diskettes, CD’s or DVD’s, manual files, handwritten notes etc, which contain personal data and are no longer required, should be treated as confidential waste and disposed of in accordance with Handling of Protectively Marked Material: A Guide for Police Personnel.

4.4.5 Where processing of police data is to be carried out by a third party on behalf of the Force, the Chief Constable must ensure that party provides sufficient guarantees in respect of the technical and organisational measures governing the processing to be undertaken.

4.4.6 This means that appropriate contractual terms and conditions will be imposed on any third party data processor to ensure that they act only on instructions given by the Chief Constable in regard to that processing.

4.4.7 Good information security is also achieved through policy and procedural controls such as the Clear Desk policy. For further guidance see relevant policies listed on the Force Intranet “Policies and Procedures A to Z pages”.

**5.** **Audit and Monitoring**

5.1 In order to ensure compliance with the [Data Protection Act 1998](http://www.legislation.gov.uk/ukpga/1998/29/contents), the Code of

Practice on the Management of Police Information and other relevant standards for the management of police information, the Chief Constable is obliged to have an audit regime to measure performance to comply with legislative and policy requirements and thereby help in endorsing the effectiveness and efficiency of operational policy.

5.2 The purpose of the Audit is to provide a systematic and independent examination to determine whether activities involving the processing of police information are carried out in accordance with the organisation’s policies and procedures and whether this processing meets the requirements of relevant legislation and standards.

5.3 A Strategic Audit Programme and annual plan will be developed from comprehensive risk analysis in accordance with the framework and standards provided by the ACPO Manual for Data Protection Management, the Data Protection Audit Manual (Office of the Information Commissioner June 2001) and the Home Office.

5.4 This will determine the nature and scope of the audit, taking into account available resources and provide a strategy which will form the basis of audit activity for the period under consideration. This Strategy will be subject to annual review and lead to a documented Strategic Audit Plan that will outline:

1. Areas to be audited;
2. Target dates; and
3. Resource allocation.

5.5 It is recognised that limited resources may restrict the number of applications or systems, which may be audited. However, the decision regarding which applications or systems will be audited, and the scope and frequency of such audit will be subject to a formal risk assessment process and current business needs.

5.6 The Strategic Audit Plan will be subject to review and approval by senior management and the Plan and associated risk analysis documentation will be

available for inspection by external audit as required.

5.7 Individual audits (as specified in the Strategic Audit Plan) will be subject to a separate planning process, with the aim of performing the audit in an effective and efficient manner. The audit plan will set out the following:

1. The scope and objectives of the audit;
2. Conduct/methodology (e.g. sample size, sample selection) of the audit;
3. Audit programme (detailing error classification and audit tests to be carried out);
4. Resource allocation and target timescales.

5.8 The Audit programme will be supplemented by quality assurance and monitoring processes undertaken by supervisors and managers in each business area.

5.9 Transaction checks will also be carried out on a regular basis in order:

1. To deter and detect unauthorised access to police information or systems;
2. To raise staff awareness of data protection issues, and maintain public confidence in the use of police information; and
3. To ensure that all required transaction fields are completed to provide an adequate audit trail for retrospective investigations into transactions that have been carried out.

5.10 Further advice and guidance is available from the Force Information Governance Manager.

**6.** **Police Systems**

6.1 **Design and Development**

6.1.1 It is the responsibility of managers and specialists responsible for the development or alteration of systems or databases for the management of police information to ensure that appropriate consultation takes place between the User, Information Services Department, Information Governance Manager and the IT Security Officer to ensure compliance with the relevant statutory provisions including:

1. [Data Protection Act 1998](http://www.legislation.gov.uk/ukpga/1998/29/contents);
2. The Computer Misuse Act 1990;
3. The Copyright, Designs and Patents Act 1988;
4. The Official Secrets Acts; and
5. The Code of Practice on the Management of Police Information.

6.1.2 All systems must also comply with relevant ACPO policy, including:

1. ACPO Community Security Policy
2. ACPO Data Protection Manual of Guidance

6.1.3 Failure to meet these requirements may lead to costly software amendments, unnecessary delays or the postponement of implementation.

6.1.4 Further advice and guidance is available from the Force Information Governance Manager and IT Security Officer.

6.2 **Operating Rules and Conventions**

6.2.1 Operating rules and conventions will be produced for national systems to establish common methods of usage and compliance for each system to which they relate.

6.2.2 Local operating rules and conventions will also be produced for the management of police information following a similar format to ensure consistency with national guidance and standards in local systems or business areas.

6.2.3 These rules define the procedures to be followed by all police personnel concerning the obtaining, use, disclosure, security and general handling of data contained in police systems. They must be read in light of the Act itself and with reference to the official details notified to the Information Commissioner.

6.2.4 The purpose of the Operating Rules is to give general guidance in the use of police information systems and also provide specific instructions in respect of individual notified purposes and compliance with the data protection principles.

**7.** **Roles & Responsibilities**

* 1. **Data Controller**
		1. The Data Controller is the person who determines the purposes

for which, and the manner in which, any personal is processed.

7.1.2 The Chief Constable is the Data Controller for the Merseyside Police.

7.2 **Data Protection Officer**

* + 1. This is a statutory duty, which in this Force is a function of the Information Governance Manager, who is responsible to the Head of the Anti-Corruption Unit. The role of the Data Protection Officer is defined in the Act and the national Data Protection Manual of Guidance and includes:
1. Ensuring that guidance is available on all aspects of the Act;
2. Ensuring that personal data held comply with the data protection principles;
3. Ensuring that compliance with the Act is maintained by providing an effective audit mechanism;
4. Conducting random sample checking of enquiries made on PNC and other force systems to ensure correct use of the data held thereon;
5. Dealing with all matters relating to subject access;
6. Promoting Data Protection awareness through training, policy development, advice and guidance.
7. Ensuring that appropriate security arrangements exists to protect data, including where necessary, that suitable contracts are drawn-up relating to the processing of police data by third parties.
8. Investigating and resolving complaints made concerning the use of data and where appropriate, assist in the investigation of disciplinary and criminal matters.
9. Liaising between the Force and ACPO Data Protection Portfolio Group
10. Liaising with the Information Commissioner.
11. Maintaining the Force’s Notification.

7.3 **Managers/Supervisors**

7.3.1 It is the responsibility of all Officers and staff who have a supervisory role to ensure that their staff operate within the terms of the [Data Protection Act](http://www.legislation.gov.uk/ukpga/1998/29/contents) , and any associated Force policies and procedural guides. This must include regular checks of work to identify training and development needs in this area and to ensure that the quality of Force information assets is of a high standard.

7.4 **All Officers/Staff/Contractors working for or on behalf of the Force**

7.4.1 There is a personal responsibility on all persons working for or on behalf of the Force to ensure that they comply with the law, Force policy and/or procedural guides when undertaking their duties. All staff must comply with the Data Protection Act regarding disclosures and exemptions with guidance contained in operating rules, conventions, policies and procedures for each system or business area.