

# **DATA PROTECTION ACT 1998**

## **Policy**

Approved by CMG on Monday, 18 September 2006



## DATA PROTECTION POLICY

### CONTENTS

<b>Policy</b>	<b>Page No.</b>
1 Policy Statement	1
2 Background to the Data Protection Act 1998	1
3 Definitions (Data Protection Act 1998)	2
4 Responsibilities under the Data Protection Act	3
5 Data Protection Principles	3
6 Rights of Individuals	4
7 Rights of Access to Data	5
8 Sensitive Personal Data	5
9 Security of Data	6
10 Disclosure of Data	6
11 Exemptions	8
12 Notification	8
13 Retention and Disposal of Data	9
14 Publication of Policing Board Data	9
15 Use of CCTV	10
16 Research	10
17 Right of Complaint	11
18 Status of the Policy	12

# DATA PROTECTION POLICY

## 1. POLICY STATEMENT

The Northern Ireland Policing Board (Policing Board) is committed to a policy of managing personal data in accordance with the following legislation:

- Data Protection (EC) Directive 1995;
- Data Protection Act 1998;
- Privacy and Electronic Communications (EC Directive) Regulations 2003;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Freedom of Information Act 2000.

The Policing Board needs to process certain information for administrative purposes (e.g. to recruit and pay individuals; to approve medical retirements). To comply with the Data Protection Act 1998, information about individuals must be collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

The policy applies to all individuals processing personal information on behalf of the Policing Board. Any breach of the Data Protection Act 1998 or the Policing Board's Data Protection policy is considered to be an offence<sup>1</sup> and in that event, the Policing Board's disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Policing Board, and who have access to personal information, will be expected to have read and comply with this policy. Directorates who deal with external agencies<sup>2</sup> will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

## 2. BACKGROUND TO THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge and, wherever possible, is processed with their consent.

---

<sup>1</sup> Offences include: Obtaining and disclosing without consent; Tampering with personal information; Not notifying; Failure to comply with a Notice served by the Information Commissioner; and Obstructing a warrant.

<sup>2</sup> Examples of external agencies used by the Policing Board are Recruitment Agencies, Medical Practitioners etc.

At present there are 24 separate sets of regulations under the Data Protection Act 1998. They include fees, tribunals, subject access, crown appointments and sensitive personal data and apply to areas such as Health, Education, and National Security etc.

The Information Commissioner, who operates as an independent public official reporting directly to Parliament, has responsibility for ensuring that public authorities comply with the requirements of all information access legislation, including the Data Protection Act 1998 (“the Act”) and has authority to take enforcement action against those which do not.

### **3. DEFINITIONS (DATA PROTECTION ACT 1998)**

#### **Data Controller<sup>3</sup>**

Any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is processed and the way in which the personal data is processed.

#### **Data Processor<sup>4</sup>**

Any person who process data on behalf of the Data Controller but, who is not an employee of the Data Controller.

#### **Data Subject**

Any living individual who is the subject of personal data held by an organisation.

#### **Personal Data**

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the Data Controller. Includes name, address, telephone number, ID number. Also includes expression of opinion about the individual and of the intentions of the Data Controller in respect of that individual.

#### **Processing**

Any operation related to organisational retrieval, disclosure and deletion of data and includes: obtaining and recording data, holding, accessing, altering, adding to, merging, deleting, retrieval, consultation or use of data disclosure or otherwise making available of data.

#### **Relevant Filing System**

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of “Relevant Filing System” in the Act. Personal data as defined and covered by the Act can be held in any format, electronic (including websites and e-mails), paper based, photographs etc from which the individual’s information can be readily extracted.

---

<sup>3</sup> The Northern Ireland Policing Board is a Data Controller.

<sup>4</sup> PWC and BMI are current examples of Data Processors of the Policing Board.

### **Sensitive Data**

This is different from ordinary personal data (such as name, address, telephone number) and relates to racial or ethnic origin, political opinion, religious belief, trade union membership, health, sex life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.

### **Third Party**

Any individual / organisation other than the Data Subject, the Data Controller or its agents.

## **4. RESPONSIBILITIES UNDER THE DATA PROTECTION ACT**

- 4.1 The Northern Ireland Policing Board as a body corporate is the Data Controller under the Data Protection Act 1988.
- 4.2 The Policing Board is committed to providing the necessary resources to ensure that data protection requirements are met.
- 4.3 The Corporate Services Director has overall responsibility for data protection. A Data Protection Officer (Compliance Manager) has been appointed with delegated responsibility for data protection. The Compliance Manager and his staff are responsible for developing specific guidance notes and providing day-to-day advice on data protection issues for Policing Board staff.
- 4.4 A Data Protection Committee (DPC) has been established to advise staff on data protection issues and provide support for the Data Protection Officer (Compliance Manager). The DPC is chaired by the Compliance Manager. It includes the Corporate Services Director, Compliance Branch staff, the Audit / IT Manager and also has representation from the Community Engagement, Planning and Policy Directorates.
- 4.5 The Senior Management Group, Heads of Branches and all those in managerial roles are responsible for developing and encouraging good information handling practice within the Policing Board.
- 4.6 Compliance with data protection legislation is the responsibility of all those staff, who on behalf of the Policing Board, process personal data. The Policing Board will ensure that:
  - All staff receive Data Protection Awareness training by means of a mandatory e-learning package;
  - Staff processing personal data will receive training in handling Subject Access Requests by means of mandatory, participative training;
  - Anyone processing personal data understands that they are directly and personally responsible for following good data protection policy and practice;
  - Queries about processing personal data are dealt with promptly and courteously;

- Methods of processing personal data are described clearly and evaluated regularly.
- 4.7 Individuals who supply the Policing Board with personal data are responsible for ensuring that it is accurate and up-to-date.

## **5. DATA PROTECTION PRINCIPLES**

All processing of personal data must be done in accordance with the eight data protection principles.

### **5.1 Personal data shall be processed fairly and lawfully**

Those responsible for processing personal data must make reasonable efforts to ensure that Data Subjects are informed of the identity of the Data Controller, the purposes(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

### **5.2 Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes**

Data obtained for specified purposes must not be used for a purpose that differs from those.

### **5.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed**

Information which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.

### **5.4 Personal data shall be accurate and, where necessary, kept up to date**

Data which is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of Policing Board staff to ensure that data held by the Policing Board is accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the Policing Board of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of Policing Board staff to ensure that any notification regarding change of circumstances is noted and acted upon.

### **5.5 Personal data shall be kept only for as long as necessary**

(See Section 13 on Retention and Disposal of Data).

### **5.6 Personal data shall be processed in accordance with the rights of Data Subjects under the Data Protection Act**

(See Section 6 on Rights of Individuals).

**5.7 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** (See Section 9 on Security of Data).

**5.8 Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data**

Data must not be transferred outside of the European Economic Area (EEA) without the explicit consent of the individual. Staff of the Policing Board should be particularly aware of this when publishing information on the internet, which can be accessed from anywhere in the globe. This is because “transfer” includes placing data on a website that can be accessed from outside the EEA.

## **6. RIGHTS OF INDIVIDUALS**

Data Subjects have the following rights regarding data processing, and the data that is recorded about them.

- To make Subject Access Requests allowing them to request a copy of all personal data held (about them) and to whom this information has been disclosed;
- To prevent processing likely to cause damage or distress;
- To prevent processing for purposes of direct marketing;
- To be informed about the “logic” behind an automated decision taking process that will significantly affect them;
- To be informed about “significant” automated decisions made about them and in certain specific cases, “not” to have the automated decision made at all;
- To sue for compensation if they suffer damage by any contravention of the Act;
- To take action to rectify, block, erase or destroy inaccurate data;
- To request the Information Commissioner to assess whether any provision of the Act has been contravened.

## **7. RIGHTS OF ACCESS TO DATA**

Any individual has the right to access any personal data which is held by the Policing Board in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Policing Board about that person.

Any individual who wishes to exercise this right should apply in writing to the appropriate branch, (see Guidance 10 on Contacts). The Policing Board reserves the right to charge a fee for Data Subject Access Requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, payment of the fee.

Staff handling Subject Access Requests will record certain information for management purposes, (see Guidance G1.9 on Recording Subject Access Requests).

In order to respond efficiently to Subject Access Requests, the Policing Board needs to have in place appropriate records management practices, (see Guidance 2 for further information on records management).

## **8. SENSITIVE PERSONAL DATA**

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Policing Board understands “consent” to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties, such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by the Policing Board (e.g. when a new member of staff signs a contract of employment). Any Policing Board forms that gather personal data should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual’s data is to be published and therefore, not gaining consent could contravene the eighth data protection principle (personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data).

If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place.

If staff require clarification about these matters, they should consult the Data Protection Officer.

## **9. SECURITY OF DATA**

All staff are responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party (see Section 10 on Disclosure of Data).

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access;
- In a locked drawer of filing cabinet;
- If computerised, password protected; **or**
- Kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as “confidential waste”. Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff processing personal data “off-site”. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing data at home or in other locations outside the Policing Board.

## **10. DISCLOSURE OF DATA**

The Policing Board must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and in certain circumstances, the police. Staff should exercise caution when asked to disclose personal data held on an individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague’s work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague’s work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is, whether or not disclosure of the information is relevant to, and necessary for, the conduct of Policing Board business. Best practice however, would be to take the contact details of the person making the enquiry and pass them onto the individual concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions applies:

- The individual has given their consent;
- Where the disclosure is in the legitimate interests of the Policing Board;
- Where the Policing Board is legally obliged to disclose the data (e.g. disability monitoring);
- Where disclosure of data is required for the performance of a contract.

The Act permits certain disclosures without consent, so long as the information is requested for one or more of the following purposes:

- To safeguard national security;\*
- Prevention or detection of crime, including the apprehension or prosecution of offenders;\*
- Assessment or collection of tax duty;\*
- Discharge of regulatory functions (includes health, safety and welfare of persons at work);\*
- To prevent serious harm to a third party;
- To protect the vital interests of the individual, this refers to life and death situations.

*\*requests must be supported by appropriate paperwork.*

When staff receive enquiries as to whether a named individual works for the Policing Board, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), staff should decline to comment. Even confirming whether or not an individual is employed by the Policing Board may constitute an unauthorised disclosure.

Unless consent has been obtained from the Data Subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the Data Subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the Policing Board may offer to do one of the following:

- Pass a message to the Data Subject asking them to contact the enquirer;
- Accept a sealed envelope / incoming e-mail message and attempt to forward it to the Data Subject.

Please remember to inform the enquirer that such action will be taken conditionally: i.e. “if the person is an employee of the Policing Board” to avoid confirming the employment of, their presence in, or their absence from, the Policing Board.

Further information regarding the disclosure of personal information can be found in Guidance 3 on Disclosure of Individuals Information and Guidance 4 on Telephone Protocol.

If in doubt, staff should seek advice from their Head of Branch or the Data Protection Officer.

## **11. EXEMPTIONS**

There are a considerable number of cases where the Policing Board may not be obliged to release information in response to a Subject Access Request.

Examples include:

- Data containing information relating to a third party for which consent to release the information cannot be obtained (see G1.4 for further detail);
- Management forecasts such as plans for redeployment, restructuring, promotions (if they would prejudice the conduct of business / activity);
- Information relating to legal proceedings being taken by the Policing Board against an individual.

For further detail, including a full list of exemptions, see Guidance 1 (G1.7).

## **12. NOTIFICATION**

Notification is the term used to describe the process by which the Policing Board registers its data holdings under the Data Protection Act 1998. It is a legal requirement that all data holdings of personal information must be notified. In practice, the Policing Board must submit specific detail of their holdings to the Information Commissioner’s office annually.

The particulars which must be notified include a description of the personal data being processed and of the categories of Data Subject to which they relate, a description of the purposes for which the data is being processed, and a description of any recipients to whom the Data Controller intends to disclose the data.

Oversight of the Data Protection Act is the responsibility of the Information Commissioner and information relating to Notification is made public on the Commissioner’s website. Notification will be the responsibility of the Data Protection Officer.

The Policing Board's Notification can be accessed via [www.ico.gov.uk](http://www.ico.gov.uk) (externally) and TRIM Record Number 45602 (internally).

Anyone who is, or intends processing data for purposes not included in the Policing Board's Notification, should seek advice from the Data Protection Officer.

### **13. RETENTION AND DISPOSAL OF DATA**

The Policing Board discourages the retention of personal data for longer than it is required. Considerable amounts of data are collected on current employees etc. However, once an individual has left the organisation, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

#### **Personal Information**

In general, electronic records containing personal information about individuals are kept as long as it is required and this information would typically include their name and address. Other information, for example, that relating to staff, will be kept by Human Resources Branch for periods stipulated in our retention and disposal schedule, for example, information relating to Income Tax, Statutory Maternity Pay etc. will be retained for the statutory time period (between 3 and 6 years).

Human Resources Branch (and other branches holding personal information) should annually review the personal information held in personal files, in electronic folders and elsewhere in accordance with the Policing Board's Records Retention Schedule (Guidance 5).

Information relating to unsuccessful applicants in connection with recruitment competitions must be kept for 12 months from the interview date unless there is an ongoing complaint in which case it may be held until the complaint is closed. Human Resources Branch (and other branches holding personal data derived from recruitment competitions) may keep a record of names of individuals that have applied for, been short-listed or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

#### **Disposal of Records**

Personal data must be disposed of in a way that protects the rights and privacy of Data Subjects (e.g. shredding, disposal of confidential waste, secure electronic deletion).

### **14. PUBLICATION OF POLICING BOARD DATA**

The Policing Board publishes a number of items externally that include personal data, and will continue to do so. These personal data are:

- The Register of Members' Interests;
- The names, roles and responsibilities of the Senior Management Team and other individuals in prominent posts e.g. Information Officers, Equality Officer.

There will be other occasions when the Policing Board wishes to publish personal information. All individuals should be offered an opportunity to "opt out" of the publication of their personal data. In such instances, the Policing Board should comply with the request and ensure that appropriate action is taken.

## **15. USE OF CCTV**

The Policing Board's use of CCTV is regulated by a separate policy.

For reasons relating to the prevention of crime close circuit television cameras are in operation inside and outside the Policing Board premises at Waterside Tower. The presence of these cameras may not be obvious. The CCTV policy, which has been approved by the Information Commissioner, determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of personnel, i.e. reception individuals;
- The recordings will be accessed only by the Compliance Manager;
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

## **16. RESEARCH**

Personal data collected for research purposes only must be processed in compliance with the Data Protection Act 1998.

Researchers should note that personal data processed for research purposes only receive certain exemptions (detailed below) from the Data Protection Act 1998 if:

- I. The data is not processed to support measures or decisions with respect to particular individuals **and**
- II. If any Data Subjects are not caused substantial harm or distress by the processing of the data

If the above conditions are met, the following exemptions may be applied to data processed for research purposes only:

- Personal data can be processed for purposes other than that for which it was originally obtained (exemption from Principle 2);
- Personal data can be held indefinitely (exemption from Principle 5);
- Personal data is exempt from Data Subject Access rights where the data is processed for research purposes and the results are anonymised (exemption from part of Principle 6 relating to access to personal data).

Other than these three exceptions, the Data Protection Act applies in full. The obligations to obtain consent before using data, to collect any necessary and accurate data and to hold data securely and confidentially, must all still be complied with.

### **Note to Researchers**

- Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes (i.e. longitudinal studies), the Policing Board recommends that, wherever possible, researchers will contact participants if it is intended to use data for purposes other than that for which they were originally collected.
- Although the Act allows for personal data processed only for research purposes only to be kept indefinitely, researchers are asked to refer to the Ethical Advisory Committee's guidelines on Data Collection and Storage.

For those branches which gather sensitive data, as defined by the Act (see Section 3 on Definitions) extra care should be taken to ensure that explicit consent is gained and that the data is held securely and confidentially so as to avoid unlawful disclosure.

### **Publication**

Researchers should ensure that the results of the research are anonymised when published and that no information is published that would allow individuals to be identified. Results of the research can be published on the web or otherwise sent outside the European Economic Area, but if this includes any personal data, the specific consent of the Data Subject must, wherever possible, be obtained.

## **17. RIGHT OF COMPLAINT**

If, following a data protection related request, an individual is dissatisfied with the response they receive from the Policing Board there is a right to make a complaint. In the first instance, the complaint must be received in writing and should be addressed to the Chief Executive at:

The Northern Ireland Policing Board, Data Protection Complaints Section,  
Compliance Branch, 5<sup>th</sup> Floor, Waterside Tower,  
31 Clarendon Road, Clarendon Dock, Belfast BT1 3BG

The complaint will be:

- Acknowledged within 5 working days;
- Reviewed by the Compliance Manager, unless he was involved in the original decision (in this instance another “Reviewer” will be nominated who will have data protection experience);
- Responded to within 20 working days from date of receipt (unless issues are particularly complex and require legal advice in which instance the complainant will be advised of a reasonable timescale).

If the problem cannot be resolved in this way, the complainant will be informed of the right to contact the Information Commissioner at:

The Information Commissioner’s Office, Wycliffe House,  
Water Lane, Wilmslow, Cheshire SK9 5AF

Telephone: 0165 545745

The Information Commissioner has the powers to investigate the complaint, and may take legal action against organisations in breach of the Act.

## **18. STATUS OF THE POLICY**

Any member of staff who considers that the policy has not been followed in respect of (1) personal data pertaining to them; or (2) personal data of others, should raise the matter with the relevant Head of Branch in the first instance, and if the issue is not resolved then with the Compliance Manager.

This policy has been screened in accordance with Section 75 equality legislation. As no significant impact on the nine Section 75 categories was identified, the policy does not require an Equality Impact Assessment.

The Compliance Manager is responsible for ensuring Policing Board compliance with the Data Protection Act 1998 and the implementation of this policy, on behalf of the Corporate Services Director.

This policy has been approved by the Policing Board’s Corporate Management Group on 18 September 2006.

This policy will be reviewed annually.