Statement on the Office's Confidentiality Strategy

This Statement is issued in conformance with the requirements set out in principle 5 of the Code of Practice for Official Statistics. It requires producers of official statistics to publish transparent guidance on their arrangements for protecting confidential data.

The Statement sets out the arrangements the Research and Performance Directorate (RPD) of the Office of the Police Ombudsman for Northern Ireland has put in place to:

- Maintain the trust and co-operation of those who own and manage the administrative Case Handling System (CHS) from which we source the data on which our statistics are based and of respondents to our surveys;

- Comply with the relevant legislation, including the Data Protection Act 1998 and the Police (NI) Act 1998;

- Comply with Principle 5 of the Code of Practice for Official Statistics, which states that: "Private information about individual persons (including bodies corporate) compiled in the production of official statistics is confidential, and should be used for statistical purposes only"; and

- Maintain the confidentiality of the data we receive, store, process and disseminate.

Requests for information

All requests for information will be dealt with in a timely manner. All requests will be treated fairly and without prejudice, taking into account the public interest, the requirements of the Data Protection Act (1998) and Freedom of Information Act (2000). Guidance on the Data Protection and Freedom of Information Acts can be found at the Information Commissioners website at www.ico.gov.uk . You can also make a request for information on the Police Ombudsman's website at www.policeombudsman.org.

Arrangements for maintaining the confidentiality of statistical data

RPD endeavours to protect all statistical data at all times, and uses a number of methods to ensure its protection.

- **Physical security**

All staff working in the organisation, and all visitors to the Office, require a security pass to access the premises. There is no public access to any part of the building where confidential statistical data may be held. Only RPD and IT support staff have access to survey data collected and to databases derived from the CHS. All paper-based survey forms are stored securely in confidential cabinets with access restricted to only those personnel who are involved in the survey production process.

- **Technical security**

Databases are held on a network drive only accessible to RPD. Personal or sensitive data are not removed from the network without the approval of the Departmental Security Officer (DSO). Electronic safeguards, such as access controls and password protected systems, are in place. No confidential statistical data are held on laptops or any other portable devices or kept on unprotected portable storage media. All transmission of data is conducted within the government information network, secure links or on encrypted e-mail.

- **Organisational security**

Data managers within the Office oversee and manage systems to protect and maintain data held by us, with the support of Information Technology professionals. The oversight roles and responsibilities the Office has in place to deliver an effective governance regime are outlined in the Office's robust security policies and include the responsibilities of all staff in the Office. Ultimate responsibility for the maintenance and delivery of this policy lies with the Director of Corporate Services, who also serves as the Office's DSO. The DSO is responsible for the accreditation of all information systems that operate in the Office and is supported by the Information Technology Security Officer (ITSO).

The Office has established an Information Risk Policy in line with the NIO Information Risk Policy and in accordance with MR32 of SPF and the Cabinet Office Guidance on data handling procedures. The Office seeks to accredit its systems in compliance with the current HMG InfoSec Standard No.2 and the Information Assurance – Accreditation Process Guidance. The Office will be guided in the accreditation process by NIO ISS.

Risk ownership resides at the very top of the Office with the Chief Executive as the Senior Information Risk Owner (SIRO) on behalf of the Police Ombudsman owning the information risk. Directors are designated as Information Asset Owners (IAO's) who will own and take responsibility for all information risks within their business area. The IAO must update quarterly the risk register including information risk. In terms of handling shared

information, the Office has Data Sharing Agreements, which endeavour to ensure that:

- ‘Access to information shall be limited to those with a ‘Need to Know’. Shared information shall be handled and stored with care, and used under conditions that make accidental or opportunist compromise unlikely and which deter deliberate compromise.
- The Office must be satisfied that the organisations with which it shares data have implemented appropriate information policies derived from a risk assessment methodology in line with the ISO27000 Standards.
- Individuals that require access to shared information must have the appropriate level of security clearance to access the information.’

All staff in the Office received mandatory data security training in 2010, alongside the internal audit and update of all related policies, serving as a timely reminder of the importance of the protection of information.

- **Disclosure Security**

RPD is aware of three types of disclosure risk in relation to the data held about individual persons, or the statistics derived from the data:

- Identity: If a person or persons can be identified (by either the persons themselves or someone else) then there is an identity disclosure risk.
- Attribute: If confidential information about a person or group of persons is revealed and can be attributed to the person, or each person in the group, then there is an attribute disclosure risk.
- Residual: If outputs from the same source, or different sources/databases, can be combined to reveal information about a person or group of persons, then there is a residual disclosure risk.

For each of our statistical and data releases, we will assess the risk of disclosure based on the following:

- Level of aggregation of the data;
- Number of tables produced from each dataset;
- Likelihood of an identification attempt;
- Size of the population; and
- Whether consequences of disclosure are outweighed through serving the public good.

As a rule of thumb, the Office will not release sensitive personal information relating to fewer than 3 individuals where that information may lead to identification of those individuals. The Office uses a number of methods to minimize the risk of disclosure. An * MAY be inserted in the relevant cell in the table with a note to indicate that this relates to fewer than 3 cases. Variable categories may also be combined or removed until only ‘safe’ cells remain.

However, the Office recognises that on occasion it may be in the public interest to publish data on certain topics pertaining to fewer than 3 individuals e.g. the number of prosecutions recommended for a certain charge, which is generally a small number.

If you have any comments, suggestions or questions about the statistics produced by the Office, we would be happy to hear from you.

You can contact us:

By letter:

Research and Performance Directorate
Police Ombudsman for Northern Ireland
11 Church Street
Belfast
BT1 1PG

By Phone:

028 9082 8670

By Email:

research@policeombudsman.org