Confidentiality and Security Strategy

The Information and Communications Unit is committed to protecting the security of our data and to uphold a guarantee that no statistics will be produced that are likely to identify any individual. This is in line with Principle T6 of the Code of Practice for Statistics. Which requires organisations to look after people's information securely and manage data in ways that are consistent with relevant legislation and serve the public good.

It sets out the arrangements the Information and Communications Unit has put in place to:

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

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

- demonstrate compliance with Principle T6 of the Code of Practice for Statistics, which states that: all statutory obligations governing the collection of data, confidentiality, data sharing, data linking and release should be followed.

Requests for information
All requests for information will be dealt with in a timely manner and should be emailed to the Information and Communications Unit at info@policeombudsman.org. All requests will be treated fairly and without prejudice, taking into account the public interest and the need to maintain confidentiality by conforming to the General Data Protection Regulation and Freedom of Information Act (2000). Guidance on Data Protection and the Freedom of Information Act can be found on the Information Commissioners website at www.ico.org.uk (opens in a new window).

Arrangements for maintaining the confidentiality of statistical data
The Information and Communications Unit aspires to best practice in the management of data and data services, including collection, storage, transmission, access and analysis. Personal information should be kept safe and secure, applying relevant security standards and keeping pace with changing circumstances such as advances in technology.

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 the Information and Communications Unit and Information Technology 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 the Information and Communications Unit and Information Technology support staff. 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 Northern Ireland Office (NIO) Information Risk Policy and in accordance with MR32 of the Sender Policy Framework 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 the risk register quarterly 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.

Staff Training
All staff working in the Information and Communications Unit are required to complete e-learning courses annually, on General Data Protection Regulation and in relation to their responsibilities for handling Information.

Disclosure Security
The Information and Communications Unit takes into account 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 three individuals where that information may lead to identification of those individuals. In such cases an * will be inserted in the relevant cell in the table with a note to indicate that this relates to fewer than three cases. However, the Office recognises that on occasion it may be in the public interest to publish data on certain topics pertaining to less than five individuals e.g. the number of prosecutions recommended for a certain charge, which is generally a small number.