Compliance with the Code of Practice for Official Statistics and Principals : Supporting Principal 5 on Confidentiality

Sections:

1. Confidentiality

This statement sets out the arrangements the National Records of Scotland (NRS) have put in place to:

- protect the security of our data holdings;
- uphold our guarantee that no statistics will be published that are likely to identify an individual unless specifically agreed with them;
- at the same time obtain maximum value from these micro-data by extending access to bona-fide and authorised third parties.

2. Arrangements for maintaining the confidentiality of statistical data

Data are held in accordance with the Scottish Government's Information Technology (IT) Policy, approved by the Scottish Government Information Systems Security Committee (ISEC) and the NRS Information Security Policy. This sets out the framework within which NRS will develop, implement, manage and review its information security. The NRS Information Systems Security Policy exists within and develops upon the Scottish Government's Information Policy.

NRS follows the Scottish Government's Information Management Principles available on the Scottish Government's website. All NRS staff will comply with the policies described above and with the Code of Practice on Access to Scottish Government Information and the Scottish Government's IT Code of Conduct, and will observe all statutory obligations and relevant codes of practice in relation to the protection of confidentiality and the handling of personal data.

Our Data Protection Policy sets out our commitment to safeguarding the confidentiality of personal data held by NRS and ensuring its fair and lawful processing, in compliance with the Code. All staff undertake mandatory annual training on their obligations under the Data Protection Act (1998).

NRS will carry out Privacy Impact Assessments (PIAs) for any project involving personal data which we consider could then have an impact on an individual's expectations of privacy and will publish the PIAs on our websites.

In every case where confidential statistical records are exchanged for statistical purposes with a third party, NRS will prepare written data sharing agreements which protect confidentiality and cover the requirements under this Code. NRS will keep an operational record to detail the manner and purpose of the processing.

3. Physical security

All staff working in this organisation require a photographic security pass and PIN to access the premises in accordance with the NRS Security Passes Policy. This covers permanent and temporary staff as well as contractors and consultants with the necessary Baseline Personnel Security Standard (BPSS) clearance. All ad-hoc visitors who are not in possession of a pass must be signed in and accompanied at all times. The public do not have access to any server area where confidential statistical data may be held. Visitors will not be allowed unsupervised access to confidential or disclosive data.

4. Technical security

We maintain a Public Services Network (PSN) compliant network. No confidential statistical data are held on laptops or any other portable devices without approved access control or kept on unprotected portable storage media. All transmission of micro-data is conducted within the PSN network or on encrypted e-mail or password protected CDs or memory sticks, which are sent by registered post.

5. Organisational security

As per the requirements of the 2008 Government Data Handling Review, the Information Asset Owner (IAO) is responsible for ensuring the management of risks to their information assets. The role of the IAO is to understand what information is held and in what form, how it is added and removed and who has access and why. NRS adopts a number of ways to limit the access to sensitive data including Access Control Policies (ACPs). ACPs document who has what level of access to which data and are implemented by the Information Communications Technology (ICT) Server teams on instruction that the ACP has been amended with approval of the IAO. See NRS Access Control Policy.

6. Disclosure Security

We use a combination of data manipulation and/or statistical disclosure techniques to meet the confidentiality guarantees. This particularly applies to:

1. Data from the Census for which the Registrar General for Scotland has given an undertaking to every person that the information they provide is treated in strict confidence.
2. Data from the National Health Service Central Register (NHSCR) on the movement between NHS Board areas of people on General Practioner (GP) patient records.

3. Disclosure security in the Census is reviewed every time a new Census is conducted. However, the statistical disclosure control methods applied to the 2011 census were targeted record swapping and table redesign to minimise small cells.
4. Disclosive Census data cannot be released for 100 years. Anyone who has access to unit record level census data must sign the census confidentiality undertaking (CCU).

7. Arrangements for providing controlled access to micro-data

For the 2011 census, we have released three micro-data products:

1. Teaching file – This file contains anonymised records on a limited set of variables for a random sample of one per cent of people in the 2011 Census output database for Scotland. It is published on the Scotland's Census website and is open to everyone.
2. Two safeguarded files - both files are five per cent sample of individuals (one at Scotland level and the other at grouped Local Authority) available from UK Data Service to approved researchers via specific end-user license arrangements. However, there will be a reduced level of detail available in the safeguarded product, reflecting the associated access arrangements and the paramount need to preserve the confidentiality of personal census information on individuals.
3. Secure files - A 10 per cent sample of individuals and a 10 per cent sample of households. These samples do not overlap and provide the most detail for the characteristics included. They are only available in a secure setting, currently the Virtual Microdata Laboratory (VML) managed by Office for National Statistics (ONS). In order to gain access to the data an application would need to be submitted and approved by the data providers and signed contracts and licence agreements are required.

Access to other micro-data may be provided to bona fide researchers in the academic sector, local and central Government and the Health Service where appropriate criteria are met under arrangements described in a Service Level Agreement, a Concordat, contracts, and confidentiality declarations. In every case, a prospective customer must sign an Data Access Agreement (DAA) to comply with the conditions for access. The management team also maintains the definitive documentation of all access to data held by the organisation.

Two projects involving use of census micro-data by external researchers are in progress:

1. Ethnicity and Health in Scotland, led by University of Edinburgh, and
2. The Scottish Longitudinal Study, led by the University of Edinburgh.

Both projects involve the linking of census records to external administrative data. All processing and analysis is done in a controlled safe setting in the NRS offices in Edinburgh.

8. Recording the details of access authorisations

Full details of all authorised access to our micro-data are available on request from the management team for each dataset or survey. Access is strictly controlled and managed on a need-to-know basis.

9. Auditing of beneficiaries of access

All beneficiaries of access are required to agree to audits of organisational, technical procedural, and physical security. The standards must be those to which the beneficiary agreed in the data access agreement.

10. Records Management

NRS manages official statistics in accordance with relevant public records legislation and codes of practice on records management, including the Public Records (Scotland) Act 2011 and the Scottish Ministers Code of Practice on Records Management by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 (Section 61 Code of Practice). The Records Management Plan of the Registrar General for Scotland and Keeper of the Records of Scotland sets proper arrangements for the management of our records.

Official statistics (accompanied by information about their purposes, design and methods) will be transferred to NRS' archives.

11. Freedom of Information

NRS follows the Scottish Ministers Code of Practice on the Discharge of Functions by Scottish Public Authorities under the Freedom of Information (Scotland) Act 2002 (Section 60 Code of Practice). Through our publication scheme and on our website we have set out the official statistics we routinely publish. We will make available information requested by an applicant or to explain why the information is being withheld.

12. Security practices

NRS has its own Information Assurance and Security team who provide authoritative advice and guidance, in line with Her Majesty's Government (HMG) Information Assurance standards and security best practice, to all personnel and contractor who work with or have access to NRS information.

Current Scottish Government and NRS practices uphold Principle 5 of the Code of Practice for Official Statistics (data identifying individuals will be kept physically secure).

13. Variations in the role of the National Statistician

The Code of Practice for Official Statistics Principal 5 on Confidentiality contains references to the National Statistician or Chief Statistician in a Devolved Administration in respect to any exceptions, required by law or thought to be in the public interest, to the principle of confidentiality protection. In respect of data produced by or for NRS all matters will be determined by the Registrar General for Scotland, carried out in a manner which is consistent with the principles of the code of practice. Final decisions on the interpretation of the standards for confidentiality will be made by the Registrar General for Scotland. The National Statistician's and the Scottish Government’s Chief statistician’s advice will be sought where necessary, and they may pursue issues should they wish under the terms of the National Statistics Framework and Statistics Concordat.

February 2016