

## **STATEMENT OF COMPLIANCE WITH THE NATIONAL STATISTICS CODE OF PRACTICE AND PROTOCOLS**

<b>1. Data Access and Confidentiality .....</b>	<b>2</b>
<b>2. Arrangements for maintaining the confidentiality of statistical data.....</b>	<b>2</b>
<b>3. Physical security .....</b>	<b>3</b>
<b>4. Technical security .....</b>	<b>3</b>
<b>5. Organisational security.....</b>	<b>3</b>
<b>6. Disclosure Security.....</b>	<b>3</b>
<b>7. Arrangements for providing controlled access to micro-data.....</b>	<b>3</b>
<b>8. Recording the details of access authorisations .....</b>	<b>4</b>
<b>9. Auditing of beneficiaries of access .....</b>	<b>4</b>
<b>10. Security practices .....</b>	<b>4</b>
<b>11. Variations in the role of the National Statistician .....</b>	<b>4</b>

## **1. Data Access and Confidentiality**

This statement sets out the arrangements the General Register Office for Scotland (GROS) 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 IT Policy, approved by the Scottish Government Information Systems Security Committee (ISEC) and the GROS Information Security Policy. This sets out the framework within which GROS will develop, implement, manage and review its information security. The GROS Information Systems Security Policy exists within and develops upon the Scottish Government's Information Policy.

All GROS staff will comply with the Information Management Policies which include compliance with the Code of Practice on Access to Scottish Government Information, the Scottish Government's IT Code of Conduct and Statutory and Regulatory requirements. These include the Data Protection Act (1998) and the Freedom of Information (Scotland) Act 2002:

- <http://www.gro-scotland.gov.uk/freedom-of-information.html>
- <http://www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=3639205>

Guidance given to Scottish Government and GROS staff on Information Management is available at:

- <http://www.scotland.gov.uk/About/FOI/19260/18444>

### **3. Physical security**

All staff working in this organisation require a pass to access the premises in accordance with the GROS Security Passes Policy. All visitors must be signed in and accompanied where appropriate on all sites. There is no public access to any part of the organisation where confidential statistical data may be held.

### **4. Technical security**

We maintain a Government Secure Intranet (GSI) 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 GSI network or on encrypted e-mail or password protected CDs or memory sticks, which are sent by registered post.

### **5. Organisational security**

We use a combination of survey project managers, data custodians, and data management teams to protect and maintain our data.

### **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 GP patient records.

Disclosure security in the Census is reviewed every time a new Census is conducted and consideration is currently being given as to the appropriate method to be used in the 2011 Census.

### **7. Arrangements for providing controlled access to micro-data**

We release micro-data, which has been made anonymous, to authorised researchers in the academic sector via the 2001 Census Sample of Anonymised Records (SARs), which is currently accessible from four Office for National Statistics sites.

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 during 2008/09:

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

## **9. Auditing of beneficiaries of access**

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

## **10. Security practices**

The Scottish Government, on behalf of GROS, is working towards compliance with the security practices related to the British Standard on Information Security Management (ISO 27001) but current practices uphold Principle 7 of the National Statistics Code of Practice Protocol on Data Access and Confidentiality (data identifying individuals will be kept physically secure).

## **11. Variations in the role of the National Statistician**

The National Statistics Protocol on Data Access and Confidentiality contain references to the National Statistician in respect to setting standards for confidentiality, designating responsible statisticians, auditing data access to third parties and having any breach of confidentiality reported to them. In respect of data produced by or for GROS all matters will be determined by the Registrar General for Scotland, although they will ensure that this is carried out in a manner which is consistent with the principles of National Statistics. Final decisions on the interpretation of the standards for confidentiality will be made by the Registrar General for Scotland. The National 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.

March 2008