# 6 Confidentiality, security and privacy

## Confidentiality principles

6.1 The White Paper on the 2011 Census in England and Wales (*Helping to shape tomorrow*)[1] noted that achieving maximum coverage in the census required public participation to be mandatory. This in turn obliged the Government to ensure that the information given in confidence by the public is treated with the strictest confidentiality. The statutory requirement to provide personal census information was prescribed by the Census Act 1920 and in the Order and Regulations made under the Act. The Act – now strengthened by the confidentiality provisions of the Statistics and Registration Service Act 2007 (SRSA) – also imposed strict requirements on the UK Statistics Authority (Statistics Board), and consequently on ONS, to protect the confidentiality of such information.

6.2 ONS recognises that the public need to be confident that their personal census records are held securely. As in previous censuses, assurances were given to the public that all the information provided would be treated in strictest confidence and that ONS would uphold its long-established reputation for maintaining census confidentiality.

6.3 The information collected in the 2011 Census is used solely for the production of statistics and statistical research. Usage complies fully with the Census Act, the Statistics and Registration Service Act and the requirements of data protection, freedom of information, and human rights legislation (see paragraphs 6.6 to 6.17). There are legal penalties for the unlawful disclosure of personal information collected in the census.

6.4 ONS ensures that government-wide standards relating to information risk management and data security are met. The following principles governed the treatment of the information given in the census returns.

1. Only persons under the management and/or control of the UK Statistics Authority including those agents acting, or providing services, on its behalf for the purpose of the census**,** and researchers approved under the provisions of the Statistics and Registration Service Act 2007 (SRSA), had access to personal census information

2. In most cases one questionnaire covered all members of the household and information was returned by post; people could choose to give personal information on a separate questionnaire or via the secure census online, in a way that would not reveal it to others in their household or establishment, or to the collector

3. All members of the census organisation and outside agents providing services to the UK Statistics Authority were given strict instructions, and were required to sign undertakings in the form of declarations, to ensure their awareness of their statutory confidentiality obligations. They were (and continue to be) liable to prosecution for any breaches of the law

4. The physical security of personal census information held in the census office, by field staff or by authorised agents, is strictly enforced. All sites where the processing of census data was carried out had continuous security

arrangements in place including access control, CCTV, security guards, intruder alarms, ONS staff to monitor suppliers, and independent checks by an accredited UK security organisation of physical and electronic security

5. All relevant UK government security requirements applicable to a RESTRICTED rated project/system were (and are) adhered to in all areas to ensure the overall security of IT systems, processes and procedures. Such measures conform to the mandatory requirements in the procedures for the handling of personal data within government

6. The computer systems handling census data have strict safeguards to prevent unauthorised access

7. There were (and are) systemic modifications of the data in the preparation of the results of the census in order to preserve statistical confidentiality (see paragraphs 6.36 to 6.44).

6.5 The security and confidentiality arrangements covering the collection and processing of census questionnaires were subject to an independent review (see paragraphs 6.50 to 6.56).

## Legislation

6.6 The confidentiality of personal census information is protected by several pieces of legislation: the Statistics and Registration Service Act 2007 (SRSA), the Census Regulations, Data Protection Act, the Freedom of Information Act, the European Convention on Human Rights, and EC regulations on European statistics.

*Statistics and Registration Service Act*

6.7 The Statistics and Registration Service Act 2007 (SRSA) makes it a criminal offence for a member or employee of the United Kingdom Statistics Authority (referred to in the Act as the Statistics Board, of which ONS is the executive arm) to disclose personal information held by the Authority in relation to any of its functions. This covers personal census information. The maximum penalty is 24 months' imprisonment or a fine or both. Section 39 deals with the duties of the UK Statistics Authority concerning the confidentiality of all personal information held by it. This states that it is illegal to disclose personal information, except in a number of specific circumstances, where disclosure is decriminalised rather than empowered. This means that any person disclosing data under these circumstances would not face criminal proceedings, but does not mean that any such disclosures must take place. The ONS policy is to refuse all requests for release of personal data.

6.8 This policy was tested in a judicial review in 2012 when a claimant asked for a declaration from the Birmingham Administrative Court stating that Section 39 4(f) of the Statistics and Registration Service Act 2007 (SRSA) was incompatible with Article 8 of the European Convention on Human Rights (ECHR) and that the policy did not properly comply with the Data Protection Act 1998 (DPA). The High Court judge in the case assessed the UK Statistics Authority's current policy on disclosure and ruled that the policy complied fully with the ECHR. The judge also dismissed the arguments that the UK Statistics Authority does not follow the DPA correctly and that therefore the current policy and practice is unlawful, in regard to:

- not providing sufficient information to people whose data are collected and held by the UK Statistics Authority about how these data are used, and
- not informing people whose data are requested to be disclosed prior to any disclosure

6.9 The ruling went on to state that there was no need for the UK Statistics Authority to inform a data subject that a request has been made for disclosure of their personal information, but that the UK Statistics Authority should tell people about how their data are used. The judge was of the view that the information that ONS puts on its website is more than enough for data subjects to read, should they wish to do so, to inform them about the uses made of their personal data. Data subjects could also ask the Information Commissioner to investigate any practices that they were unsure of or uncomfortable with.

*Census Regulations*

6.10 The Census Regulations (see paragraphs 2.366 to 2.374) prescribed measures to ensure the security of the completed questionnaires and confidentiality of the data in the field. The sections described below relate to both the Census (England) Regulations 2010[34] and the Census (Wales) Regulations 2010[35].

6.11 Section 14 related to the giving of information and was concerned about the confidentiality of personal information given to the 2011 Census field staff; it prescribed that any person:

*'…to whom personal information is given in accordance with these Regulations must not without lawful authority -*

*(a) make use of that information; or*
*(b) publish it or communicate it to any other person.'*

6.12 Section 15 was concerned with the safe custody of questionnaires and documents, and prescribed that:

1) *'Any person having custody, whether on their own behalf or on behalf of any other person, of questionnaires or other documents (including electronic documents) containing personal information relating to the census must keep those documents in such manner as to prevent any unauthorised person having access to them.'*

2) *'When directed to do so by the Authority, any appointee must send the Authority all records in that appointee's possession (including any electronic record) which contain personal information relating to the census.'*

3) *'The Authority must arrange for the secure storage of questionnaires, electronic storage devices, or other documents containing personal information relating to the census.'*

6.13 Section 16 set out the provisions for all field and data processing staff to make statutory declarations or sign undertakings which required that they would not, except in the performance of their census duties, disclose or make known, now or at any

time after, any matter which came to their knowledge relating to any person, family or household.

*Data Protection Act*

6.14 In addition to the protection afforded by the census-specific legislation referred to above, the Data Protection Act 1998 (DPA) specifies that, where personal data are processed on behalf of the 'data controller' (ONS in the case of the census), that data controller is responsible for ensuring that any contractor processes them in accordance with the data protection principles. Accordingly, ONS provided its contractor with instructions to ensure that this happened.

*Freedom of Information Act*

6.15 Information collected from the 2011 Census (and from all censuses from 1921) is protected from the general disclosure provisions of the Freedom of Information Act 2000 by Section 44 of the Act, which exempts such information if disclosure is prohibited by or under any enactment. ONS frequently relies on this exemption in order to protect personal data in response to freedom of information requests.

*European Convention on Human Rights*

6.16 Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms concerns the rights of freedom of expression and the rights of citizens to

'….*hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers*'.

However, where confidentiality is concerned, Article 10 says that these freedoms, carry with them duties and responsibilities, and so may be subject to such

'… *formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society for preventing the disclosure of information received in confidence*'.

6.17 Article 8 concerning the 'right to respect for private and family life', affords further protection regarding confidentiality of information:

*'Everyone has the right to respect for his private and family life, his home and his correspondence'.*

However, the UK and European courts have ruled that the census itself does not infringe this right, because the article goes on to state that:

*'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.*

*EU statistical legislation*

6.18 The UK is required to make data available by a European Union (EU) regulation to provide comparable statistics and transparency about the quality of census outputs across all EU member states (EU Regulations 763/2008[4], 519/2010[5] and 1151/2010[76]).

6.19 The European Commission has a number of regulations concerning the confidentiality of European statistics, in particular *Commission Regulation (EC) 223/2009* on access to confidential data for scientific purposes, and *Commission Regulation (EC) 831/2002* on the transmission of data, subject to statistical confidentiality, to the Statistical Office of the European Communities (Eurostat). Consequently the UK census data that are provided to the EU are completely anonymised and protected against disclosure using techniques that apply to all other census outputs (paragraphs 6.36 to 6.44). In addition, all of the information provided to the EU has been rounded to the nearest five.

6.20 To ensure transparency, each member state is also required to provide a quality report to Eurostat. This includes definitions, legal acts covering the collection of the census, confidentiality policies, and a list of statistics that have been published from the census. Section 7 of this quality report concerns confidentiality and sets out the UK's policy on confidential data.

## Security measures

6.21 Data security is a top priority for the census. In addition to the strong protection provided by the law (described above), ONS put in place stringent additional safeguards.

*Data and systems security*

6.22 All staff who process census data are security cleared. This requirement was extended to all employees of the contracted supplier and their sub-contractors who handled any personal census data during the data processing operation. Staff who have access to the full census data set or substantial parts of it have security clearance to handle material classified as 'Secret'.

6.23 Underlying security requirements for census data are based on UK Government security guidelines issued by the Cabinet Office and by the Communications Electronic Security Group (CESG), the UK Government's National Technical Authority for Information Assurance which assists government departments with their own communications security. Furthermore, the census security programme is managed to the framework of ISO 27001, the internationally recognised Information Security Management Standard.

6.24 Census data are classified as 'restricted' under the Security Policy Framework, the government's information classification scheme. This classification brings a set of standards and safeguards which ensure that data remain secure. This includes control of physical access to any site or room where the data are kept, secure control of access to IT hardware and of course IT systems.

6.25 ONS controls system access rights to all systems and data. All security measures cover the completed questionnaires, the electronic data set, the website, the archive

image system and the communications links relating to any of these items. All of the electronic communications links used for routing personal census information are encrypted (scrambled) to the levels recommended by the Government Security Services.

*Security and external suppliers to the census*

6.26 As noted at paragraphs 2.332 to 2.335, ONS carried out a fully compliant procurement, in accordance with European law and the European Union Procurement Directives, to source a range of support services for the 2011 Census. Lockheed Martin UK was selected as the main contractor.

6.27 The 2011 Census White Paper '*Helping to shape tomorrow*' reported that:

'*The UK Statistics Authority is satisfied that ONS has fully addressed concerns about the security and confidentiality of census data arising from the involvement of Lockheed Martin UK*'[1].

However there was some public concern about the possibility of the United States Patriot Act being used by United States intelligence services to access confidential data collected in the census.

6.28 Consequently, ONS put in place additional contractual and operational arrangements to ensure that US authorities could not gain access to census data. These ensured that:

- all data processing was carried out in the UK
- ONS would retain custody of the data at all times
- only people who worked for ONS had access to the full census dataset in the operational data centre
- no staff from Lockheed Martin UK (the contracted supplier) or Lockheed Martin (the US parent company) would have access to any personal census data
- ONS controlled access rights to all data systems
- everyone working with census data signed declarations of confidentiality, and
- independent checks by an accredited UK security consultancy of both physical and electronic security were carried out

6.29 The prime contractor was Lockheed Martin UK Ltd. Additional specialist services were provided by Cable and Wireless, Logica, UK Data Capture, bss, Steria, Polestar, Oracle and Royal Mail. Lockheed Martin UK designed the processing systems for ONS using its expertise and experience. However, the day-to-day running of operational services was provided by the consortium of specialist service providers. All of these specialist subcontractors were registered and owned in the UK or elsewhere in the EU.

*Alleged breach of security*

6.30 In June 2011 some media stories alleged a breach in the security of census data. The notorious hackers LulzSec claimed that they had gained access to the full census database. ONS immediately confirmed that the security measures in place were more than adequate to protect the public's confidential data. A press briefing

was issued on 22 June explaining that personal census information was secure and the allegation that it had been hacked was a hoax. The hackers subsequently admitted that this was the case.

## Online security

6.31 Security was, of course, a fundamental aspect of the 2011 Census, and was built into the whole of the census design. The online census, in particular, was built with data security as a primary requirement and met government information assurance and data security standards, as well as ISO 27001, the industry standard for information security management.

6.32 The online census was subject to rigorous security tests, and underwent a formal accreditation process before it went live. In addition to the security testing by Logica, ONS commissioned its own independent security testing by consulting specialists SOPRA - a service provider accredited by CESG.

6.33 The method of security used to protect the confidentiality of census data transmitted over the internet from individual PCs to the ONS servers was SSL. ONS installed EV certificates issued by Verisign. ONS were verified by Verisign as the certified issuing authority. Steria, an ONS subcontractor, was the authorised holder of the private keys installed on the systems load balancers. Servers were based at the Manchester census data capture centre, with strong physical and system security measures protecting them. No personal census data were transmitted outside the UK over the internet.

6.34 All households received a paper questionnaire before they were given the option of making their return online. There was no facility to enable a householder to pre-register an intention to respond online as the risk of failure to make a return was considered to be too high. Instead, a unique 20 digit reference number on each paper questionnaire formed the security code for accessing and completing an online return.

6.35 Particular protection was given to the information provided via the online completion system. The online questionnaire was delivered and accessed within a secure architecture with multiple layers of firewalls and intrusion detection systems that incorporated industry-leading technologies to monitor and protect against cyber attacks. This kept the personal data provided by the public confidential throughout its capture, storage and processing. All the systems were subject to security testing by two separate government-approved security testing companies, which provided independent assurance that they were secure, free from technical vulnerabilities, and had been developed in accordance with best practice.

## Statistical disclosure control

6.36 Statistical disclosure control (SDC) involves measures to support the 2011 Census confidentiality commitments that no statistics will allow the identification of an individual (or any information about an individual) with a high degree of confidence. It covers a range of methods to protect individuals, households and organisations, and their attributes (characteristics), from identification in published results (see Chapter 7). As noted above, ONS has legal obligations under the Statistics and Registration Service Act (SRSA) 2007 and the Data Protection Act 1998 (DPA) to protect the confidentiality of census data. In addition, the Code of Practice for Official

Statistics requires ONS not to reveal the identity or private information about an individual or an organisation.

6.37 The key strength of the census is its completeness of coverage and its ability to generate statistics about very small areas and groups of people (which help public policy makers to take account of local communities' needs). Particular care must therefore be taken to balance the need to ensure complete statistical confidentiality against the need to avoid damaging the utility of the data. This has always been paramount. In a census context, where thousands of cross-tabulations are generated from one database, the protection of the statistical confidentiality is best addressed by introducing uncertainty about the true value of small cells. In order to meet the agreed interpretation of the code of practice, ONS, together with the other two UK Census Offices, agreed that small counts could be included in publicly disseminated census data provided that:

- uncertainty as to whether or not the small cell is a true value has been systematically created, and
- creating that uncertainty does not significantly damage the data

6.38 Following the Treasury Select Committee's recommendation to review the mechanism to protect statistical confidentiality[6], ONS took steps to ensure a high degree of confidence that no statistics would be produced that allowed the identification of an individual (or information about an individual).

6.39 There are a variety of statistical disclosure control methods available that can be applied to census data before the statistics are released such as:

- restricting the number of output categories into which a variable may be classified, such as aggregated age groups
- amalgamating any small area in which the number of people or households falls below a minimum threshold, with a neighbouring area such that the threshold for the combined area is exceeded, and
- modifying some of the data through one or more of a variety of means such as record swapping, over-imputation and some form of cell perturbation

6.40 Some 13 different SDC methods were initially compared in order to discount those methods that would not be able to satisfy the strict disclosure control requirements for 2011 Census outputs. The short-listed SDC methods were assessed using a risk-utility framework. Record swapping was recommended as the primary disclosure control method for 2011 Census. This recommendation was accepted by the ONS Statistical Policy Committee, and endorsed by the UK Census Committee in 2009.

6.41 In the method adopted, every individual and household was assessed for uniqueness or rarity on the basis of a small number of characteristics, and every household given a risk score. A sample of households was selected for swapping. The chance of being selected in the sample was based largely on the household risk score, so that households with unique or rare characteristics were much more likely to be sampled. However every household had a chance of being swapped. Once selected it was swapped with another 'similar' household from another area.

6.42 Households in the 2011 Census were usually swapped only within local authorities; households with very unusual characteristics were swapped with matches in nearby authorities. So, for example, a household in Cornwall would not be swapped with one

in Birmingham. As every household had a chance of being selected for swapping, there is a level of doubt as to whether a count of one in any cell is real. It may be that a person has been imputed or swapped so as to appear in that cell; or there may have been another person or persons swapped out of that cell, thus creating a count of one. So no one can ever be absolutely sure that a value of one that they see in a table is really the true value.

6.43 Before publication, each census output table is assessed to ensure there are no disclosure issues. At this stage any necessary disclosure can be further managed by restricting the design and complexity of the tables, by collapsing variable categories, or by raising geographical thresholds.

6.44 Links to the documents **'***Statistical disclosure control for 2011 Census'* and **'***Confidentiality protection provided by statistical disclosure control'* are available on the ONS website[49]. Further SDC related links on the topic of **'***Protecting confidentiality with statistical disclosure control***'** are available at the webpage[49].

## Privacy impact assessment

6.45 Projects that involve collecting personal information inevitably give rise to privacy concerns. A privacy impact assessment (PIA) is a self-assessment process developed by the Information Commissioner's Office (ICO) to help organisations foresee the likely privacy impacts on individuals and to weigh these against the benefits to society in the collection, use and (secure) disclosure of information.

6.46 The PIA process was introduced by the Information Commissioner around 2009, and so the 2011 Census programme was already well established before the PIA process was published. There is no legal requirement to carry out a privacy impact assessment. However, it is a legal requirement for everyone in England and Wales to participate in the census, and it is recognised that some members of the public have concerns over privacy, so ONS carried out a full-scale PIA for the 2011 Census. Because privacy and confidentiality are of prime importance to ONS, most of the good practice in the PIA process was already well established in the 2011 Census programme, needing only to be collated into a single document.

6.47 Different types of privacy impact are possible depending on the scale and nature of the project. ONS carried out a full-scale PIA which covered an in-depth internal assessment of privacy risks and liabilities. ONS sought advice from the Information Commissioner's Office on the scope of the PIA. Given that a census has been carried out decennially since 1801, the advice was to focus on those aspects of the 2011 Census which were new and had been introduced since the 2001 Census.

6.48 The Information Commissioner's Office suggested that a number of organisations and individuals representing privacy concerns/interests be invited to a meeting on the census and privacy in June 2009, or asked to make representations in writing. The main concerns raised as a result were:

- justifying the need to collect any census information at all, and
- the publication of census results to ensure that individuals were not identifiable

6.49 The PIA was published[50] in November 2009 and focused on:

- considering the need for a 2011 Census, and whether or not there were alternative ways of providing census-type information
- the legal basis for the census
- the questions to be asked, especially those new to the census, and the analyses of the acceptability of the questions
- equality impact assessments and considerations
- the use of third parties, and how privacy concerns were addressed in supplier contracts
- security and confidentiality considerations regarding the 2011 Census operations (such as the online census, questionnaire tracking, decommissioning and destruction of information after the census), and
- measures to ensure that individuals are not identified in the published results

## Independent reviews of security and confidentiality

6.50 Security and confidentiality have been reviewed and reports published by ONS (and its predecessors) for each census since 1981. For the 2011 Census, and in light of the increased public concern about the security of personal information generally, ONS invited an independent team to review in detail the arrangements in place to ensure the security and confidentiality of census data. The independent information assurance (IA) review was undertaken in two phases.

6.51 The first phase started in March 2010 and reviewed the arrangements and undertakings in place prior to the census up to mid-December 2010. It was published in February 2011 (in advance of census day) and covered issues such as:

- the legal framework
- questionnaire development
- the 2009 rehearsal and lessons learned
- printing, distribution and data collection
- online response
- support to the public
- support to the census operations
- the census quality survey
- data processing
- end users of the data
- contractual arrangements
- management of information assurance

6.52 The key conclusions of the review, published on the ONS website[51] (and which in fact covered the arrangements for all three UK censuses) were that:

- there was a sound basis of commitment, knowledge and personal responsibility underpinning the information security management aspects of the 2011 Census operations
- there was solid management resolve towards ensuring that the 2011 Census should build upon previous experience in securely managing census operations and data

- the assurances given to the public by the census office regarding the US Patriot Act were consistent across the legal and operational arrangements set in place with its commercial partners. The issues of potential access to census data under the Patriot Act had been well addressed
- there had been a significant increase in the level of public awareness of data security and the need for demonstrable protection of personal information. Against that background ONS had risen to the challenge of implementing effective information security as part of its census operations
- online data gathering was expected to account for approximately a quarter of the total number of returns (in the event it was just 16.4 per cent). The review team were satisfied that the information assurance measures put in place for this relatively new aspect of census operations were appropriate and could be expected to be effective
- the review team made suggestions for improvement, mostly in terms of achieving greater consistency across the three census operations. These were welcomed by ONS, and the short timescales in which the suggestions were implemented demonstrated both commitment and capability, and
- ONS had undertaken assurance activities not just as a matter of adopting a professional approach and implementing best practice, but as a crucial part of the preparation for the census

6.53 The review team noted in their report that ensuring the protection of personal information provided by the public had been a core objective from the outset in planning the 2011 Census. The review team had had the opportunity to thoroughly review planning, management and implementation aspects, with the full co-operation of the staff involved, and had had complete access to 2011 Census staff, sites and documentation.

6.54 The reviewers concluded that:

'*As a result of our review, we are very satisfied that the three census offices are managing Information Assurance pragmatically, appropriately and cost-effectively. We are, therefore, confident that they are capable of delivering their IA objectives and that information will be held in secure environments and that it will be handled in line with best practice and Government standards. The public can be assured that the information they provide to the 2011 Censuses will be well protected.'*

6.55 The aim of the second phase of the review, which covered the period from the initial report to the first release of census data in July 2012, was to build on the earlier findings by examining the evidence relating to:

- the operations undertaken immediately prior to census day
- the census activities themselves, and
- the secure decommissioning and archival activities which marked the end of the data collection process

6.56 The final report of the review team was published on the ONS website in June 2012[51], and concluded (in referring to all the census offices) that:

'*As a result of our review, we are very satisfied that the IA operations undertaken by each Office were matched to their business objectives and business environment, and that as a result, the personal census data gathered and handled by each was subject not only to an adequate degree of protection, but also to a degree of*

*protection which was appropriate to individual circumstances. It is clear to the review team that the tightly focused work undertaken by each organisation has had benefits not only across the three Census Offices, but also across Government, and that the benefits will be felt for some time to come…*

*…this has probably been the most rigorous census in terms of IA ever conducted in the UK. The fact that there have been no significant security incidents in the course of the project to date is not simply a matter of good luck. It is a reflection of sound IA planning, which has been well implemented in the form of an effective through-life approach. We remain satisfied, therefore, that the public can be assured that the information they have provided to the 2011 Census has been well protected and that sound plans are in place to ensure that this will continue to be the case'.*