Office for National Statistics

The Census and Future Provision of Population Statistics in England and Wales: Privacy Impact Assessment for the Initial Research Stage

March 2015

Table of Contents

Executive Summary

A Privacy Impact Assessment (PIA) is a process designed to assess and manage privacy risks associated with the collection, use and disclosure of personal information. The preparation of this document takes account of guidance issued by the Information Commissioner's Office[1] as well as the advice of privacy advocates and covers the initial research stage of work on 'The census and future provision of population statistics in England and Wales'. The information set out here will need to be reviewed and revised to take account of our ongoing programme of research as well as decisions relating to plans for an online census in 2021 and the increased use of administrative and survey data. Further details on the overall scope of this document, specific inclusions and exclusions are set out in Section 1 ('Background and Introduction').

The document takes account of early work undertaken as part of the Beyond 2011 Programme to review requirements and options for the future provision of population statistics and the next census in England and Wales. This included consideration of users' requirements for population statistics (Section 2), research on various approaches to counting the population (Section 3), an extensive programme of stakeholder engagement and consultation (Section 4) as well as research into public attitudes to the use of personal data (Section 5).

Our consideration of privacy risks has been informed by the development of a risk assessment framework. This is designed to provide an objective basis for identifying, managing and mitigating privacy concerns associated with specific statistical activities from initial data collection to the dissemination of statistical outputs, the storage and retention of data. Details of the measures that have been, or will be, taken are set out in Sections 6.1 to 6.7.

PIAs should be seen as an integral part of a privacy by design approach as well as a basis for ensuring that full and proper account is being given to statutory obligations such as those in the Census Act 1920, the Statistics and Registration Service Act 2007 and the Data Protection Act 1998. These aspects of our work are covered in Section 7.

This PIA covers the initial research phase of our ongoing programme of work. In accordance with guidance issued by the Information Commissioner's Office it will be reviewed and amended as work proceeds and more detailed decisions are made. The Office for National Statistics (ONS) is committed to safeguarding the confidentiality of all the information that it collects and processes to produce and publish statistics. Updated PIAs will be produced so that stakeholders, users and members of the public can be assured that full account has been taken of the need to protect all personal data and protect privacy. As a result this PIA should be viewed as a living document which will be revised and updated as detailed

[1] 'Conducting Privacy Impact Assessments Code of Practice', Information Commissioner's Office, February 2014.

decisions on an online census and the increased use of administrative and survey data are taken.

Feedback on this initial PIA is very welcome; ideas, advice and comments may inform future work and privacy considerations.

1 Background and Introduction

Purpose of Privacy Impact Assessment

1.1 A Privacy Impact Assessment (PIA) is a process designed to assess and manage privacy risks associated with the collection, use and disclosure of personal information. PIAs help identify and address privacy concerns. In accordance with recommendations arising from the Government's Data Handling Review[2] the Office for National Statistics (ONS) [3] must complete such assessments for both new and existing policies. In addition, such assessments are necessary in order to comply with requirements in the Data Protection Act 1998 and the Statistics and Registration Service Act 2007 as well as commitments specified in our Information Charter.

1.2 The general public have shown a growing awareness of privacy issues over the last few years. They are concerned about the amount and type of information being collected and shared, the nature and pace of technological innovation as well as some high profile losses of personal information. Consequently, any recommendation for meeting future requirements for population and small area socio-demographic statistics needs to be publicly acceptable. ONS has a duty to explain the measures being taken to safeguard the confidentiality of any data it may collect or use for census or related purposes.

Scope of the report

1.3 This initial PIA covers work being taken forward by the Beyond 2011 Programme on the future provision of population statistics in England and Wales and forms part of our risk management processes. It demonstrates our commitment to safeguarding confidentiality and working in an open and transparent way. Where relevant, account has been taken of previous PIAs developed to support work on the 2011 Census and applications for access to data from administrative sources.

1.4 In view of the nature of the work being undertaken and advice from the Information Commissioner's Office, ONS is carrying out a full-scale privacy impact assessment. This necessitates an in-depth internal assessment of privacy risks and liabilities, consultation with users and other stakeholders as well as the development and implementation of measures to manage or mitigate any issues of specific concern.

[2] 'Data Handling Procedures in Government: Making Government Work Better', Cabinet Office, November 2008.

[3] The Office for National Statistics, the executive office of the UK Statistics Authority, is responsible for the collection, compilation, analysis and dissemination of a range of economic, social and demographic statistics about the UK.

1.5 This PIA should be seen as a living document which will be updated and amended as work proceeds over the coming years. This is consistent with the general rationale for such assessments which emphasise the need for, and importance of, an iterative approach. Such an approach is essential in order to respond effectively to new or revised policy drivers, changes to our work plans, methods or approaches and technological advances as well as wider legislative, data security or handling requirements. This initial review records our understanding of current issues and comments on the further work that will be carried out.

Aims and objectives

1.6 In all cases any work which makes use of personal data must be appropriate and proportionate. The primary aims of this assessment are to demonstrate that we have:

- a clear and comprehensive understanding of any privacy risks or issues raised by stakeholders, users, data suppliers or members of the public
- developed measures to manage, mitigate or accept specific risks
- taken full account of our statutory obligations and ethical standards

1.7 In considering these issues special attention will be given to the rationale governing the overall programme of work. Further details relating to what will, or will not, be covered in this initial assessment are outlined below.

Inclusions

1.8 This review is focused on the research being carried out to assess the best way of meeting future requirements for population and small area statistics in England and Wales[4]. Special attention has been given to:

- explaining the need for, and the importance of, our research and methodological work
- understanding users' requirements for statistics
- identifying privacy risks and issues associated with public acceptability and attitudes to data sharing
- describing the processes we have put in place to manage and mitigate current risks
- highlighting the issues that will need to be considered as we take forward the National Statistician's recommendation to make the best use of all sources, combining data from an online census in 2021, administrative data and surveys

[4] ONS is responsible for the census in England and Wales. In Scotland and Northern Ireland these duties are carried out by the National Records of Scotland and the Northern Ireland Statistics and Research Agency.

Further work required

1.9 At this stage no detailed decisions have been made on the processes or procedures that will be required to take forward and implement the National Statistician's recommendations and further work will be required to consider issues such as:

- the extent of data linkage and integration of data from administrative and survey sources
- the privacy provisions that should be put in place for such linkage building on the arrangements made for the research phase of the programme. Further details are available in the paper 'Safeguarding Data for Research: Our Policy' published in July 2013
- any new or improved safeguards (over and above those implemented for the 2011 Census and the research phase of the Beyond 2011 Programme) that may be required to deal with privacy concerns associated with online data collection and plans to make more use of administrative data

What is privacy?

1.10 The Information Commissioner's Office has identified four different aspects of privacy namely:

- the privacy of personal information
- the privacy of the person
- the privacy of personal behaviour, and
- the privacy of personal communications

1.11 In this case safeguarding the privacy of personal information, that is 'data privacy' or 'information privacy', is the most important issue. This covers all activities associated with the production and dissemination of statistics including data collection, data processing as well as quality assurance and validation procedures. Individuals need to know that their data will be safe and secure, who will have access to their information and how it will be used.

1.12 All work undertaken by ONS is governed by statutory requirements and specific ethical obligations including those set out in the Code of Practice for Official Statistics[5]. Our work depends upon the good will and support of individuals and as a result the maintenance and preservation of privacy underpins everything that we do.

[5] UK Statistics Authority, Code of Practice for Official Statistics, January 2009.

1.13 The other aspects of privacy identified by the Information Commissioner's Office which include 'privacy of the person'[6], 'privacy of personal behaviour'[7], and 'privacy of personal communications'[8] are not applicable to the work we are undertaking. Further details on the different dimensions of privacy are set out in Chapter Two of the Privacy Impact Assessment Handbook published by the Information Commissioner's Office.

What do we mean by 'privacy risks'?

1.14 In view of concerns about the use of personal information, the increasing application of new technologies and some well publicised breaches of data security, ONS is committed to demonstrating that all the data that it accesses, collects or uses meet its statutory objective 'of promoting and safeguarding the production and publication of official statistics that serve the public good'[9] and that all work is carried out with due regard for privacy. This report sets out the measures that have been taken to identify and address privacy risks or issues associated with the Beyond 2011 Programme, not least those associated with:

- ensuring that full and proper regard is being given to individuals' rights to privacy
- protecting the data that we access and use
- preventing the abuse or misuse of data
- avoiding accidental or deliberate disclosure of data or any data losses

1.15 The assessment of risks to individual privacy must be complemented by consideration of organisational risks. Any breach of privacy would have serious repercussions for both the work and reputation of ONS.

1.16 As the work is at an early stage there are still many uncertainties and therefore this document will be reviewed and updated as decisions are made and more detailed plans are developed and implemented. Assessing privacy risks and issues is an ongoing activity and as a result we anticipate that further iterations of this document will be produced and published.

[6] 'Privacy of the person' covers activities such as body searches, biometric measurement and the provision of samples of body fluids or tissue.

[7] 'Privacy of personal behaviour' relates to the observation of what individuals do, including systematic observation, the recording or transmission of images and sounds.

[8] 'Privacy of personal communications' includes the analysis, recording, interception or monitoring of communications.

[9] s.7(1) Statistics and Registration Service Act 2007.

2 Users' Requirements for Population Statistics

2.1 For over 200 years the United Kingdom (UK) has relied on censuses to underpin national and local decision making. Although the amount and type of information produced has varied in response to changes in users' requirements, three basic types of information are provided routinely:

- counts of population units (people, households and dwellings)
- details on family and household composition
- socio-demographic and housing statistics - including details on employment, economic activity, travel to work, ethnicity, health, qualifications and tenure as well as other characteristics

2.2 The census for England and Wales provides consistent and comparable statistics on the demographic, social and economic circumstances of the population from the national to the local level every 10 years and supports the cross tabulation of data on different topics. A special feature of the census is that these statistics are published for very small areas (covering about 125 households and 250 people on average) as well as for very small sub-groups of the population.

2.3 Obtaining the best quality statistics for government and other users is essential and the Beyond 2011 Programme has undertaken an extensive programme of consultation to ensure that it has an accurate and up-to-date understanding of ongoing requirements. A summary of our main findings is outlined below.

Changes in user requirements for statistics

2.4 Our assessment of users' requirements took the work carried out for the 2011 Census in England and Wales as a starting point. The summary details outlined in this document are based on: the results of two public consultations[10], research and discussion with experts, groups of users and nominated departmental and local authority representatives as well as workshops and presentations.

2.5 Changes in requirements need to be understood in the context of changing policy priorities as well as wider economic and social circumstances. In particular, users have commented on the impact of new legislation, including requirements set out in the Child Poverty Act 2010, the Equalities Act 2010, the Localism Act 2011, the Welfare Reform Act 2012 and the Health and Social Care Act 2012, as well as organisational and administrative changes. Other relevant factors include general societal changes, not least those associated with increased mobility and ageing.

2.6 Although overall requirements have increased some topics have gained in importance and others have become less significant. For example, increasing

[10] 'Beyond 2011 User Needs Consultation', ONS, 17th October 2011 - 20th January 2012 and consultation on 'The Census and Future Provision of Population Statistics in England and Wales', ONS, 23rd September - 13th December 2013.

demands for information on household and family structure, migration, the labour market and socio-economic data have been complemented by a greater need for data on ethnicity, national identity, language, religion and, to a lesser extent, health and disability.

2.7 Despite the increased availability of some information from administrative sources, there is a demand for information on additional topics such as household income, digital inclusion/exclusion, energy efficiency, sexual orientation, volunteering and charitable work. Further details are available from the 'Beyond 2011 User Requirements Consultation Report' published in August 2012.

Ongoing needs

2.8 Population and socio-demographic statistics continue to be needed for a range of purposes including resource allocation, service planning and delivery. Their importance has been emphasised by new policy priorities including the drive for greater efficiency, accountability and transparency.

2.9 Central government, local authorities, the health sector, businesses, market researchers, voluntary and charitable organisations, genealogists and the public rely on census statistics for a range of purposes. Summary details on core requirements are outlined below:

- **Public and private sector funding and resource allocation** - population counts and other characteristics from the census are used to support applications for funding, to allocate resources and to target investment at both national and local level. It is essential that all such decisions are based on consistent and comparable data.

- **Service planning and delivery** - the drive for greater efficiency and effectiveness has increased the need for reliable population statistics to help commission, plan and target public services. Details on size and structure as well as detailed living arrangements are essential if we are to understand the increasingly complex ways in which people live, plan the infrastructure and deliver the services that people need.

- **Policy making, monitoring and review** - the ongoing commitment to evidence-based policy making, the emphasis on localism and the drive for efficiency have increased the need for accurate and reliable socio-demographic data at the community and local level. For example, better information is needed to respond to major challenges such as those associated with an ageing population, monitoring and managing migration, meeting housing needs, promoting equality and social cohesion.

- **Academic research** - the availability of consistent and comparable data from a national to a local level, combined with the ability to produce

multivariate statistics, is vital for research to identify and assess the impact of demographic and other social trends. Data are used directly and indirectly to investigate area characteristics, understand change over time, delineate labour market areas, develop indicators and other statistical measures.

- **Market research** - census data are used to develop strategies and plans, support decision making and associated investment, target campaigns or promotions, identify and understand local markets. Small area data are especially important for the construction of non-standard geographies.

- **Genealogical and social research** - covers those with an interest in family history as well as those undertaking social or historical research. The retention and preservation of an historical record at household and family level will be required for these purposes.

2.10 Furthermore, census information provides the basis for the derivation of the annual mid-year population estimates and is used to improve the quality of many other statistics. Data taken from the census, or based on it, are used to select areas in which to conduct research, as control variables for statistical or econometric analysis and for weighting and grossing surveys.

2.11 A 'Summary of the uses of census information' was published by ONS in September 2013.

2.12 A second public consultation was carried out from September to December 2013 to seek the views of users on two approaches for census taking in future and to consider the amount and type of information that each could provide. The results[11] substantiated the ongoing need for, and value of, census information.

[11] 'The Census and Future Provision of Population Statistics in England and Wales: Report on the Public Consultation', ONS, March 2014.

3 Census Approaches

Scope and purpose of the Beyond 2011 Programme

3.1 The 2011 Census successfully provided population statistics that will be used for the next ten years by planners, policy makers and researchers across the public and private sectors. After each census ONS reviews the future needs for information about population and housing in England and Wales and how these needs might be met.

3.2 In recent times it has become more challenging and expensive to conduct censuses and household surveys in developed countries, partly because of the complexities associated with an increasingly mobile population but also because of a general decline in the public's willingness to take part. At the same time, users want a greater range of outputs to be available and updated more frequently in order to have a better understanding of the population and how it is changing.

3.3 ONS set up the Beyond 2011 Programme to consider the best way of meeting future requirements for population and socio-demographic statistics in England and Wales by assessing the relative merits of a number of alternative approaches. Special attention has been given to considering the possibilities associated with improvements in technology as well as making better use of data already held within government.

Summary of the work

3.4 Research began in April 2011. An initial list of possible approaches for producing population and socio-demographic statistics in England and Wales was drawn up including:

- full census
- short form and long form census
- short form census plus continuous survey
- rolling census
- address register plus survey
- administrative data - aggregate
- administrative data - record linkage
  - partial linkage
  - 100% linkage

3.5 A summary description of these options is provided in the report 'Beyond 2011: The Options Explained' (paper M1, published in October 2012).

3.6 The Programme has adopted an iterative approach to its research, using evaluation criteria such as statistical quality, cost, technical and legal feasibility, public acceptability and burden, to review each option and exclude those that did

not meet specified standards (e.g. the required level of detail or quality). A number of the initial options were discounted, including the short form and long form census, aggregate analysis of administrative data and the partial linkage of administrative data as well as the address register and survey option. The remaining approaches were revised and refined to take account of specific design decisions, most notably those associated with the size and frequency of the survey needed to provide attribute data. This work is described in more detail in the paper 'Beyond 2011 Options Explained 2' (Paper M3, published February 2013).

3.7 The subsequent assessment was based on a revised shortlist of approaches including:

- full census - taken every 10 years as previously but modernising our approach to give much more emphasis to internet data collection
- rolling census - an annual census of up to 10 per cent of the population carried out in different areas each time
- short form census and 4 per cent annual survey
- annual linkage and 10 per cent 10-yearly survey
- annual linkage and 4 per cent annual survey
- annual linkage and 40 per cent 10-yearly survey

3.8 Outcomes from the evaluation carried out during the summer of 2013 are set out in 'Beyond 2011: Options Report 2' (Paper O2, published in July 2013). An overview of the work is available from 'Beyond 2011: Narrowing Down the Options' (Paper O3, published November 2013).

3.9 Our research and assessment resulted in two potential approaches for census taking in future:

- once a decade, like that conducted in 2011, but primarily online, and
- using existing administrative data and compulsory annual surveys

3.10 The issues and implications associated with these findings, including descriptions of each approach, their strengths and weaknesses, risks and opportunities and the statistics each method would provide, were set out for public consultation, 'The census and the future provision of population statistics in England and Wales', which ran from September to December 2013. The consultation documents can be found here.

3.11 The main findings from this consultation were that:

- there was continuing demand from government, local authorities, public bodies, business, the voluntary sector and individual citizens for detailed information about small areas and small populations offered by the decennial census, whether online or paper-based

- there was a strong concern that the proposed use of an annual survey of 4 per cent of households (to support the use of existing administrative data) would not meet these needs, nor deliver the required small area and small population statistics offered by the decennial census
- the more frequent statistics that could be provided between censuses by the use of administrative data and annual surveys would be welcomed, but not at the expense of the detailed statistics
- whilst the methods using administrative data and surveys show considerable potential, there was concern that these were not yet mature enough to replace the decennial census
- many respondents proposed a hybrid approach, making the best of both approaches, with an online census in 2021 enhanced by administrative data and household surveys

3.12 As a result of this feedback, the findings of an independent review of methodology[12] and external research into public attitudes[13] to the census and data sharing, on 27 March 2014 the National Statistician recommended:

- an online census of all households and communal establishments in England and Wales in 2021, as a modern successor to the traditional, paper-based decennial census. As in 2011, ONS recognises that special care would need to be taken to support those who are unable to complete the census online, and

- increased use of administrative data and surveys in order to enhance the statistics from the 2021 Census and improve statistics between censuses.

3.13 The Government has endorsed[14] the National Statistician's recommendation stating that:

- "we agree with the recommendation for an online census in 2021 as a modern successor to the traditional paper-based decennial census, with support for those who are unable to complete the census online"

- "we welcome the increased use of administrative data in producing the census in 2021 and other population statistics, and to improve statistics between censuses, since this would make the best use of all available data and provide a sound basis for the greater use of administrative data and surveys in the future"

- "we welcome ONS plans for further research to determine the most appropriate blend of methods and data sources for the 2021 census

[12] 'Beyond 2011: Independent Review of Methodology', Chris Skinner, John Hollis and Mike Murphy, October 2013.

[13] Reports on the Beyond 2011 Public Attitudes Research published in May 2014 can be accessed here.

[14] Letter from the Rt. Hon. Francis Maude MP, Minister for the Cabinet Office to Sir Andrew Dilnot, 18th July 2014.

However, our support for the dual running of an online (decennial) census with increased use of administrative data is only relevant to 2021 and not for future censuses."

3.14 ONS will be taking forward the work to consider these requirements.

4 Stakeholder Engagement and Consultation in England and Wales

4.1 The 2013 public consultation was the culmination of extensive stakeholder engagement activities over the past three years. The Beyond 2011 Programme's strategy for stakeholder engagement has been informed by a commitment to:

- engage and debate with all those with an interest in our work on the future provision of population statistics
- be open and transparent
- present information in an accessible and innovative way

4.2 Our programme of engagement and consultation has been designed to:

- explain the programme's aims, progress and plans
- understand users' current and future requirements
- communicate the issues and implications associated with any new model;
- ensure that any recommendation takes account of our duties to safeguard privacy and is acceptable

Stakeholder engagement activities

4.3 As described previously, the Programme has undertaken two major consultations:

- **17 October 2011 - 20 January 2012** - focused on understanding users' current and potential future requirements, the relative importance of frequency, accuracy and geography, and identifying any data sources that could contribute to the production of the required population statistics. Further information is available here. Some 266 organisations and individuals provided responses to the consultation and 207 attended the supporting workshops. The information they provided facilitated the development of the assessment criteria and evaluation of alternative approaches.

- **23 September 2013 - 13 December 2013** - asked all those with an interest in the future provision of population statistics to comment on two potential approaches for taking the census in future and to consider their advantages, disadvantages and risks. A series of documents including an online questionnaire were published to support the consultation which received 712 responses, and more than 500 people attended various public events or meetings.

4.4 From the outset the need for direct engagement and ongoing dialogue with privacy and other advocacy groups was recognised. The measures adopted included:

- **bilateral discussions** - with representatives of organisations working to defend privacy, civil liberties and human rights including Big Brother Watch,

Liberty and Privacy International. These activities have been complemented by ongoing negotiations with individual data suppliers and consultation with the Information Commissioner's Office

- **establishing a Privacy Advisory Group** - members include Big Brother Watch, Privacy International, Open Rights Group and Oxford Internet Institute. Regular updates on progress and plans have been provided either via face-to face or audio meetings. Members have been asked to comment on the measures we are taking to protect privacy, to review papers and to comment on plans for managing privacy risks and related issues

- **engaging with technical experts** - our data processing and research facilities have been accredited by independent experts including a consultant (approved under the Communications-Electronics Security Group Listed Advisory Scheme (CLAS)). Similarly, our methods of pseudonymisation have been reviewed by a leading expert in cryptography and computer security

4.5 At the same time account has been taken of comments from users and others with an interest in the Programme as well as submissions received as part of our public consultations. In light of the Government's endorsement of the National Statistician's recommendation ONS will need to consider the best ways of ensuring that all those with an interest in the future provision of population statistics in England and Wales can contribute to our ongoing programme of work.

5 Public Acceptability in England and Wales

5.1 From the outset the Beyond 2011 Programme recognised the need for a clear understanding of public attitudes to issues such as data sharing, data linkage and the creation of linked datasets. The programme of research that has been carried out has enabled us to understand the factors affecting public opinion, to identify specific risks and issues of concern.

5.2 A summary of the work that has been done over the period 2009-2013 including findings from the quantitative and qualitative research undertaken by ONS, commissioned by ONS and carried out by Independent Social Research Ltd and by Ipsos MORI are outlined below:

- There is generally a very low level of public understanding about how data are collected and used and only a basic awareness of the related vocabulary
- The public generally do not understand the difference between operational and statistical uses of personal data
- The public are supportive of data sharing when personal or public benefits can be demonstrated and are communicated effectively
- Data linking and storage are more acceptable if personal data are anonymised (i.e. name, address and other personal identifiers are removed). However, explaining the process of anonymisation is complex and difficult for the public to understand
- Any objections to the use of personal data are largely related to security and privacy concerns
- The public get most of their information about the use of personal data from the media and their own personal experiences
- Public confidence in ONS is high with 78 per cent stating that they think the organisation adequately protects the confidentiality of the personal information it collects
- The public are generally positive towards the decennial census as a means of gathering information about the population
- When provided with reassurance about security and privacy, the public broadly support ONS re-using administrative data to produce statistics

5.3 The public's view of the acceptability of using personal data varies according to who is using the data and for what purpose. Although three quarters do not object to data being shared with ONS, there are concerns about data sharing in general including:

- security and confidentiality
- privacy and anonymity
- transparency, control, consent and trust
- governance and regulation
- public and personal benefits

5.4 Further details are available from the report on 'Public attitudes to the use of personal data for official statistics' published in March 2014.

5.5 In addition, there were a number of comments on privacy issues in the 2013 public consultation:

- some respondents expressed concern about hacking in relation to an online census solution
- while fewer than six per cent of respondents mentioned privacy or security in relation to the decennial census, 13 per cent commented on these issues in relation to the administrative data and surveys approach
- some respondents questioned whether it was appropriate or legal to re-use data for statistical purposes when it had been collected for other purposes, and were concerned that the quality of information provided might be affected by such actions

5.6 The 'Report on the Public Consultation' published in March 2014 provides further details.

5.7 The research[15] we have carried out shows that the public express mixed opinions about the use of their personal data for research and statistical purposes. While the majority support the sharing of data with ONS there are concerns about security and privacy which must be allayed. ONS will undertake further research to understand how the issues can be communicated effectively, to explain the differences between statistical and operational uses of personal data and the safeguards that are in place to protect privacy and confidentiality.

[15] Reports on the Beyond 2011 Public Attitudes Research published in May 2014 can be accessed here.

6 How We Have Assessed Privacy Risks

6.1 The Beyond 2011 Programme has developed a risk assessment framework to provide an objective basis for identifying, managing and mitigating privacy issues or concerns.

Assessment framework

6.2 The framework is based on understanding the interactions between our core tasks or activities and specific privacy requirements which encompass:

- legal obligations
- technical safeguards
- operational processes

6.3 All processes/procedures must comply with specific statutory obligations (e.g. those in the Data Protection Act 1998, Human Rights Act 1998, and the Statistics and Registration Service Act 2007) as well as the Code of Practice for Official Statistics and our ethical standards. At the same time appropriate technical safeguards must be applied, including both physical and technical measures, and our systems must comply with relevant standards (e.g. those specified by CESG the UK Government's National Technical Authority for Information Assurance). Finally, our operational processes (e.g. staff vetting and related procedures) must take account of the overarching need to keep all the data that we use safe and secure.

6.4 In view of the nature of the work, special attention has been given to the following:

- access to, and use of, data from administrative sources
- data collection (including the collection of population and attribute data, data for assessing coverage and quality)
- data processing (including pre-processing, data linking and matching, coverage assessment and adjustment, edit, imputation and quality assurance)
- publication/dissemination of outputs
- data retention/destruction
- decommissioning systems

6.5 Each of these activities will be considered in subsequent sections of this report.

6.1 Data Access

6.1.1 Much of the research work being carried out by the Beyond 2011 Programme requires access to data collected and held by other Government departments or public authorities. Information such as name, address and date of birth is essential for accurate linking between sources. This is a pre-requisite for assessing the feasibility of producing high quality statistics on the population of England and Wales from administrative sources. At this initial research stage attention has focused primarily on making use of information to assess and evaluate alternative methods for estimating the overall size and structure of the population. The sources include the 2011 Census, the Patient Register, Student Record and Customer Information System. Further details are set out in Table 1 (below) and Annex A.

Table 1: Sources for Initial Research

Data Source	Data Provider
2011 Census and Census Coverage Survey	Office for National Statistics
NHS Patient Register for England and Wales	Health and Social Care Information Centre
Student Record	Higher Education Statistics Agency
School Census for England	Department for Education
School Census for Wales	Welsh Government
Birth Registrations	General Register Office, Identity and Passport Service
Death Registrations	General Register Office, Identity and Passport Service
Lifetime Labour Market Database (L2) (1% sample)	Department for Work and Pensions
Customer Information System	Department for Work and Pensions, HM Revenue and Customs and the Department for Social Development (NI)
Electoral Registers	Electoral Registration Officers
e-Borders/Border Systems Programme	Home Office

6.1.2 Details of the processes and procedures we have put in place to authorise access to, and use of, the required data are considered here. Arrangements governing the collection of data via an online census and from surveys are covered in Section 6.3 on Statistical Data Collection.

Securing access to data from administrative sources

6.1.3 ONS can access and make use of data collected and held by central government departments or other public authorities only where it has the legal authority to do

so. In all cases any data made available to ONS can be used only for statistical purposes, including to:

- develop new statistics including cross-cutting statistics
- improve the quality and/or coverage of existing statistics
- provide statistical information to underpin policy development, analysis or evaluation
- reduce the costs and burden associated with the production of statistics

6.1.4 The statement of users' requirements published as part of our public consultation in September 2013, together with the series of research reports produced by the Beyond 2011 Programme,[16] demonstrate that the work we are undertaking is compatible with these specifications. In addition, ONS must comply with the Data Protection Act 1998 as well as the standards and commitments set out in the Code of Practice for Official Statistics. The processes and procedures undertaken to meet these obligations are outlined below.

(i) Clarifying the legal position - data can be shared with ONS only if it is lawful to do so, either because there are existing powers which authorise their disclosure or new provisions (Information Sharing Orders) are made.

(ii) Justifying requirements - ONS must explain how the data will be used and demonstrate that our requirements are proportionate and take account of the data protection principles in the Data Protection Act 1998 (most notably principle three which states that 'personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'). The detailed arrangements designed to satisfy these requirements vary and may include the preparation and publication of statistical business cases as well as the completion of specific departmental processes. Where relevant, the appropriate type of privacy impact assessment must be carried out. Finally, individual data sharing applications may need to be scrutinised and approved by committees such as the Data Access Ethics Committee in the Department for Work and Pensions.

(iii) Authorising disclosure - in the absence of legal powers authorising disclosure, ONS may make use of provisions (s.47) in the Statistics and Registration Service Act 2007 to develop data sharing regulations. Any such proposals can proceed only if the disclosure is in the public interest, and has the consent of the Minister for the Cabinet Office and other relevant Ministers. In all cases draft regulations must be considered and approved by Parliament by affirmative resolution. Currently four sets of regulations (Information Sharing Orders) have been passed which are relevant to the work being

[16] All reports are available on the ONS website and can be accessed here.

carried out by the Beyond 2011 Programme. Annex A provides further information about these together with details relating to access arrangements for other relevant datasets.

6.1.5 Following the Government's endorsement of the National Statistician's recommendation ONS will need to consider what additional information may be needed to ensure that we can make better use of administrative and survey data to improve population statistics. As a result we will require access to data from an increased number of administrative sources to support ongoing work on the derivation and evaluation of trial outputs covering both estimates of the population and socio-demographic characteristics. Although it is not possible to comment in any detail about specific sources, potential future requirements are set out in Table 2.

Table 2: Possible Future Requirements for Administrative Data

Topic	Potential Supplier (Department/Agency)
Core Census Topics	
Population size and structure (Activity data to facilitate assessment of location/place of usual residence and whether present or absent)	Department for Work and Pensions HM Revenue and Customs Health and Social Care Information Centre Department of Health Department for Transport Driver Vehicle and Licensing Agency
Information on Specific Characteristics	
Health	Health and Social Care Information Centre Department of Health NHS England NHS Wales Public Health England Public Health Wales Department for Work and Pensions
Education	Department for Education Department for Business, Innovation and Skills Welsh Government
Transport	Department for Transport Driver and Vehicle Licensing Agency
Housing	Valuation Office Agency Department for Communities and Local Government Welsh Government
Potential New Topics	
Income	HM Revenue and Customs Department for Work and Pensions

6.1.6 In accordance with existing arrangements the processes and procedures for any future data acquisitions will take full account of our statutory obligations and ethical standards.

6.2 Data Transfer

6.2.1 Once the legal authority to share personal data held or owned by government departments or other public authorities has been secured, arrangements must be made for the transfer of the specified information to ONS. Any movement of data from one place to another must be managed with care in order to minimise any associated risks.

6.2.2 This part of the PIA summarises the measures that have been put in place to demonstrate ONS's ongoing commitment to safeguarding confidentiality. Further details relating to the collection and transfer of data from an online census and from surveys are considered in Section 6.3 (Statistical Data Collection).

Transferring data from administrative sources

6.2.3 The processes and procedures we have put in place take account of the recommendations in the 'Data Handling Procedures in Government: Final Report' published in 2008, and comply with the detailed standards and protocols specified in the Government's Security Policy Framework and the principles set out in the Code of Practice for Official Statistics. These documents provide the basis for protecting information and managing risks effectively, collectively and proportionately. As a result ONS works cooperatively with individual data suppliers to:

- apply the correct protective marking to individual datasets
- select proportionate controls and data handling methods
- meet compliance and assurance requirements

6.2.4 In all cases the measures taken to safeguard individual datasets are based on a careful assessment of sensitivity by data owners or suppliers. Each assessment takes account of the amount (number of records) and type of information being transferred. Such details determine the level of protection required which in turn governs the security measures that need to be applied.

6.2.5 Although the processes and procedures for individual datasets may vary, in all cases the data are transferred using tried and tested methods on Communications-Electronics Security Group (CESG) [17] approved media. In cases where removable media are used these are encrypted to agreed standards and protected by an appropriate authentication mechanism for additional security. In some instances arrangements may be tailored to take account of specific legal obligations or departmental requirements. As a result it is not uncommon for ONS to have to secure formal clearance from information assurance committees (for example, the Department for Education's Data Management Advisory Panel).

[17] The Communications-Electronics Security Group is a branch of the Government Communications Headquarters working to secure the communications and information systems of the government. CESG is the UK National Technical Authority for Information Assurance.

6.2.6 The arrangements agreed, including any requirements for the use of specific software or methods of encryption together with ongoing compliance and assurance processes, are set out in detailed memoranda of understanding or service level agreements. These documents are reviewed regularly and amended or updated as necessary. In accordance with Government requirements ONS must make an annual return to the Cabinet Office covering any significant security incidents or issues including details on the actions taken to manage information risk[18].

6.2.7 ONS will continue to ensure that all processes and procedures relating to data handling and transfer take full account of any changes in statutory requirements, technical or ethical standards.

[18] ONS has not been required to report any data losses as part of this process.

6.3 Statistical Data Collection

6.3.1 This part of the PIA deals with the processes and procedures we will put in place to safeguard the confidentiality of data collected directly by ONS in order to meet its statutory obligations under the Census Act 1920 and the Statistics and Registration Service Act 2007.

6.3.2 Any proposals for the enumeration of the population via a 2021 online census or the collection of data on socio-demographic attributes using surveys would need to be authorised by Parliament and comply with legal requirements set out in the Data Protection Act 1998 and Human Rights Act 1998 as well as specific obligations specified in the Code of Practice for Official Statistics and our Survey Charter. Similarly, the methods we use to transfer any data must comply with Government standards for data handling and security including those set out in the Security Policy Framework.

Online census

6.3.3 At this stage no detailed plans have been made for taking an online census in 2021 and thus the details set out below must be treated as provisional. This PIA will need to be reviewed and revised to take account of processes and procedures which have yet to be determined.

6.3.4 The Census Act 1920 allows a census to be held, makes ONS responsible for undertaking such an exercise in England and Wales, and makes it a criminal offence for a person responsible for taking part in a census not to do so. Furthermore, the Census Act makes provision for two pieces of secondary legislation: a Census Order and Census Regulations. Further details are set out in Section 7 of this document.

6.3.5 Online data collection was introduced for the 2011 Census and 16 per cent of respondents opted to make use of the internet. The development was welcomed, with many users noting that they found online completion quick, simple and easy. Indeed, the advantages are recognised internationally by countries such as Canada, Australia and New Zealand. For example, Canada introduced use of the internet in 2006 and their subsequent census in 2011 was conducted primarily online. In a similar way decisions about an online census for England and Wales in 2021 will build on the experience gained from its successful introduction in 2011.

6.3.6 ONS commissioned an Information Assurance Review to provide an independent assessment of the protection to be applied to personal information gathered as part of the 2011 Census. The review concluded that “the public can be assured that the information they provide to the 2011 Censuses will be well protected and securely managed”. Two documents were published by the independent review team: an initial report in February 2011 and a final paper in June 2012.

6.3.7 Whatever detailed decisions are made, care will be taken to ensure that appropriate security measures are built into the system to safeguard the confidentiality of the information provided by respondents, counteract threats from hacking or attempts to disrupt the system or deface the website. Advice will be provided to respondents to protect their privacy and security.

6.3.8 Layers of security will be built into the online questionnaire to:

- check that interactions are authentic (i.e. check that the access code supplied is valid)
- protect the information
- detect and deter deliberate or accidental interference
- verify the security of the website and its authenticity (i.e. enable the respondent to verify, and ONS to demonstrate, adherence to security standards/requirements)
- transfer the information to ONS securely

6.3.9 For the 2011 Census the following processes and procedures were used to protect the collection and transfer of data via an online questionnaire:

- **Internet Access Code** - access to a questionnaire was based on the unique internet access ID used to create it. This code acted like a password, limiting access and protecting against fraudulent submissions and malicious actions

- **Encryption** - to safeguard confidentiality during the completion of the questionnaire. Any information exchanges between the respondent and the online server were encrypted thus protecting all interactions from deliberate or accidental interference

- **Digital certification** - certification of the site to reassure users about its authenticity and secure status (included verification of the organisation which owns the digital certificate, the issuing organisation and the dates for which the certificate is valid)

- **Security** - special attention was given to the security of the web host, its infrastructure, staff vetting and security procedures including accreditation and access controls

- **Transfer to ONS** - secure data transfer arrangements were made

6.3.10 Whatever methods are put in place for the 2021 Census, respondents may be confident that full and proper attention will be given to physical and information system security as well as issues of availability. Detailed design and security decisions will take advantage of technological advances, new or improved standards and techniques (e.g. standards for online security or methods of

encryption) and so the specified measures may be adapted or changed. All systems will be subject to independent testing and accreditation.

6.3.11 We can anticipate that any internet facilities will include the following core components:

- an online census questionnaire
- online help facilities including reassurance and advice for members of the public about maintaining the confidentiality of their data
- the ability to request materials

6.3.12 ONS recognises that special care will need to be taken to support those who are unable to complete the census online. Appropriate measures will be taken to support full participation and take account of the requirements of those without access to broadband or a computer, as well as those with special needs.

6.3.13 Decisions relating to the topics to be included in the online census have yet to be agreed. In accordance with previous practice there will be a programme of consultation, question development and testing to ensure that each question provides good quality outputs, and to consider issues such as public acceptability and respondent burden.

6.4 Data Processing

6.4.1 All data handling and processing arrangements must comply with the Government's Security Policy Framework which provides the basis for assessing and managing risks and protecting information assets. At the same time it will be important to ensure that the processes and procedures we put in place meet specific statutory requirements as well as the standards set out in the Code of Practice for Official Statistics. Details relating to possible plans for an online census, use of administrative and survey data are outlined below.

Online census

6.4.2 No detailed plans have been made for a census in 2021 and therefore the processes and procedures considered here must be treated as provisional and subject to amendment and revision. As with arrangements for the 2011 Census appropriate safety and security measures will be put in place for the capture, transfer and processing of census data in 2021.

6.4.3 ONS will be able to draw on the expertise of its staff and the experience it has accrued from the successful conduct of previous census operations. As in 2011 any arrangements for capturing and processing census data will comply with government-wide standards for information assurance, data security and risk management, including those promulgated by CESG and the International Organization for Standardization (ISO)[19].

6.4.4 It is likely that ONS will make use of some form of questionnaire tracking system in order to monitor response and follow up any outstanding returns. In common with procedures adopted in 2011 it is likely that each address will have a unique identifier. Although no decisions have been made about what information would be held on the questionnaire tracking system we can anticipate that, in common with procedures for the 2011 Census, only information to support the census operation would be required.

6.4.5 The design of any census will require a comprehensive high quality address register for all areas in England and Wales. ONS is evaluating the suitability of AddressBase[20] but may need to make additional arrangements to supplement this in order to meet specific quality and coverage requirements. In all cases access to, and use of, any address based products will be carried out in accordance with our legal obligations and ethical standards, most notably those associated with safeguarding the confidentiality of any personal information. Detailed terms and conditions would be set out in service level agreements (see Section 6.1 for further details).

[19] International Organization for Standardization is an independent, non-governmental organisation developing and promoting standards covering electrical, electronic and related technologies as well as other products, services and systems.

[20] AddressBase is a national address product developed by Geoplace, a public sector limited liability partnership between the Local Government Association and Ordnance Survey.

6.4.6 ONS will ensure that the computer systems and communication networks used in connection with the collection or processing of data will meet government security standards and reflect the volume, nature and sensitivity of the information being handled. Systems will be independently tested and accredited as appropriate in accordance with government standards.

6.4.7 Appropriate technical measures will be complemented by stringent physical security, rigorous procedural arrangements and personnel controls. For example, only authorised and appropriately cleared staff will be permitted to access, or work with, census data.

6.4.8 At this stage we do not know whether or not all of the data will be processed on ONS premises. However, in common with previous practice special attention will be given to the transfer of any data. Any processes or procedures that may be put in place will take full account of any changes in the mandatory security measures required by the Government, new or improved software, removable media or other devices. The current position is that, at a minimum, we would adopt measures similar to those put in place for the 2011 Census. This means that statistical data would always be transferred via secure encrypted media.

6.4.9 While ONS will be responsible for, and run, any future census in England and Wales, its core competencies relate to methodological, statistical and operational issues including question testing, questionnaire design, statistical processing, coverage assessment and adjustment, validation and quality assurance. As a result it is likely that other activities may be outsourced to specialist external providers including private companies.

6.4.10 ONS successfully outsourced census services in 1991 (e.g. publicity, distribution), in 2001 (e.g. postal services, questionnaire printing, questionnaire scanning, data capture and coding as well as the census call centre and helpline) and in 2011 (e.g. publicity, questionnaire printing, postal services, questionnaire scanning, data capture and coding, census helpline, field staff recruitment, payment and training). Any proposals for outsourcing services for a 2021 Census would be conducted in accordance with government procurement standards and requirements, designed and managed to safeguard the confidentiality of personal information and to deliver value for money. In all cases steps will be taken to ensure that they apply and enforce the same security and privacy standards.

6.4.11 ONS will be responsible for drawing up the detailed specification of requirements for any contracts. Any companies bidding for work would be subject to the same mandatory security standards and information assurance procedures (including the independent testing and accreditation of systems) which apply to work carried out by ONS. Furthermore, all staff working on the census, whether ONS employees or contractors, must comply with relevant legislative requirements,

including those set out in the Statistics and Registration Service Act 2007 (e.g. provisions in s.39)[21] and the Data Protection Act 1998. It is likely that, as for the 2011 Census, all census staff, ONS employees and contractors, would be required to sign a confidentiality undertaking confirming that they understand their obligations and are aware of the penalties associated with any infringement.

Administrative and survey data

6.4.12 The Beyond 2011 Programme has tried and tested procedures in place to safeguard the confidentiality of the data being used for our current research. The measures are based on a comprehensive assessment of risk and take full account of our legal, security and ethical obligations. All our systems and processes are designed to:

- provide the right level of protection
- minimise the scope for error or malicious action

6.4.13 In accordance with the Government Security Policy Framework a range of robust security controls is in place to meet physical, technical and procedural requirements. Further details relating to the measures we have put in place for the research phase of the programme are outlined below and in the paper 'Safeguarding Data for Research: Our Policy' published in July 2013.

(i) Physical - a Statistical Research Environment (SRE) has been designed to store and process all the information being used for our research. The SRE has been designed specifically to address the privacy and security concerns that may arise when statistics are produced using data from multiple administrative sources. As work progresses arrangements may need to be made to deal with information collected from surveys in combination with data from an increased number of administrative sources.

The SRE is located on an ONS protected site. It may be accessed only by authorised and security cleared researchers, data processing and security staff. All access is recorded, monitored and regularly audited by ONS Security Managers by reviewing technical, procedural and CCTV records. As a result any unauthorised activities will be identified and dealt with appropriately. This could include prosecution for anyone found to have contravened any of our statutory obligations.

Measures have been put in place to ensure that all the data we access and use is protected appropriately. More specifically, arrangements comply with the terms and conditions set out in our service level agreements with individual data suppliers, with mandatory government standards, and our statutory responsibilities.

[21] Section 39(9) - anyone found guilty of disclosing personal information will be liable to a term of imprisonment not exceeding two years, or to a fine, or both.

(ii) Technical - the SRE is fully isolated from all other systems and networks whether external or internal to ONS. Within the environment, technical safeguards exist to ensure only authorised research can take place. Any 'unusual' activity is detected, assessed and acted on. Unauthorised devices, software or connections are not permitted in the SRE under any circumstances and protective measures are in place to enforce this policy.

The SRE has been assessed, tested and fully accredited in accordance with requirements specified by CESG to store, process and protect the data currently being used for research purposes by the Beyond 2011 Programme. Arrangements are in place to ensure that the accreditation is reviewed as necessary to take account of any future data acquisitions.

(ii) Procedural - all data management, import and export processes are carried out by independent ONS staff (that is individuals who are not working for the Beyond 2011 Programme). All processes are subject to strict controls which include a clear and distinct separation of duties to ensure that no single individual would be able to subvert any procedure.

The SRE is managed and run by staff with the highest level of security clearance. All researchers working within the environment are ONS employees and are security cleared in accordance with National Security Vetting standards. All operations within the SRE are supervised by independent security managers with the appropriate level of security clearance. In accordance with agreed standards regular reviews are undertaken to reassess and confirm the security status of relevant staff.

In accordance with government requirements all staff receive regular security training and are required to sign the ONS Confidentiality Declaration to confirm that they understand their obligations to keep information safe and secure and the penalties associated with any infringement of our statutory and other related obligations[22].

6.4.14 In accordance with arrangements agreed with individual data suppliers the SRE facility and our operational practices may, at short notice, be subject to independent audits or inspections.

6.4.15 At present the SRE is designed to store, process and protect all the data currently being used by the Beyond 2011 Programme as well as future updates of data from specified administrative sources or systems (see Annex B). As further administrative data sources are identified, and the work is extended to

[22] The Confidentiality Declaration is designed to cover legal requirements set out in the Statistics and Registration Service Act 2007, the Data Protection Act 1998, the Code of Practice for Official Statistics and ONS's policies and Standards for confidentiality and information security.

consider the application and use of survey data, security and privacy arrangements will be reviewed.

Statistical processes

6.4.16 The SRE is used for all research and statistical work being carried out by those working for the Beyond 2011 Programme. At present this includes the following tasks or activities:

- pre-processing (i.e. initial quality checks, standardisation and geo-referencing of key variables, derivation of new variables, creation and addition of match keys, transformation (hashing of identifiable information - see paragraph 6.4.19 below and Annex B for further details))
- production of summary statistics that cannot be created after data transformation (e.g. distribution of month of birth)
- data linkage and matching
- production of statistical population datasets
- coverage assessment and adjustment
- derivation of trial outputs (currently population estimates at local authority level but in the longer term will include details for smaller areas as well as estimates for a range of socio-demographic characteristics)
- validation and quality assurance of statistical outputs
- disclosure checks

6.4.17 In view of the nature of the work being undertaken by the Beyond 2011 Programme special attention has been given to the processes and procedures associated with the linking and matching of data from multiple sources in order to minimise any associated risks and demonstrate our ongoing commitment to safeguarding confidentiality and security.

6.4.18 The arrangements we have put in place are designed to reduce any privacy risks to an absolute minimum. As a result all research work carried out on the Beyond 2011 Programme uses pseudonymised data. All uniquely identifiable fields within each dataset are hashed. To further protect the data this work is carried out by an independent team on a separate IT system which is physically disconnected from, but still part of, the SRE.

6.4.19 At present we are using a cryptographic hash function (SHA-512) designed by the US National Security Agency to anonymise person identifying information including names, dates of birth and addresses. The hash function, which converts a field into a condensed representation of fixed value, is a one-way process. Once the hashing algorithm is applied it is not possible to get back to the original information without significant effort. The methods have been reviewed by CESG and discussed with members of the Beyond 2011 Privacy Advisory Group and officials from the Information Commissioner's Office.

6.4.20 A detailed specification of the cryptographic functions currently being used is set out in Annex B. Further details on our matching are available from a number of published papers including 'Beyond 2011 Matching Anonymous Data'. It should be noted that this innovative work has been commended in the report completed as part of the Beyond 2011 Independent Review of Methodology commissioned by ONS.

6.4.21 Future arrangements for data processing and the derivation of statistical outputs will be a key part of our work going forward. Whatever decisions are made full account will be taken of government standards and accreditation processes. ONS will be able to draw on the work carried out to safeguard the 2011 Census data as well as experience associated with the running of the SRE.

6.5 Production and Publication of Statistical Outputs

6.5.1 ONS has considerable experience in assessing disclosure risk, developing and implementing appropriate methods to safeguard confidentiality whilst minimising the impact on the utility and quality of any outputs. As the largest independent producer of official statistics in England and Wales, ONS publishes a multiplicity of statistics derived from census, survey and administrative sources.

6.5.2 Results from an online census or derived from multiple sources must meet users' requirements and be accessible. Any outputs produced and disseminated by ONS must be non-disclosive in order to comply with requirements to protect confidentiality set out in the Statistics and Registration Service Act 2007 (s.39) and the Code of Practice for Official Statistics.

6.5.3 Census statistics that we produce in future could be delivered in new and innovative formats and disseminated in a number of ways. ONS has an exemplary record of safeguarding confidentiality. In all cases appropriate disclosure control methods will be applied to ensure that we continue to uphold our commitments to protect privacy.

6.5.4 In accordance with previous practice ONS will adopt a range of techniques to modify or summarise the data in order to reduce the risk of disclosing any personal information. The strategies and methods that are likely to be applied could include some, or all, of the following:

- restricting the number of output categories into which a variable may be classified (e.g. by aggregating age groups)
- amalgamating data in cases where the number of people or households in an area falls below a minimum threshold
- modifying some of the data before the statistics are released, using 'record swapping' (records with similar characteristics are swapped with a record from another geographic area)

6.5.5 In cases where the impact of disclosure control may damage or limit the usefulness of the data (e.g. more detailed tables), special access arrangements may be put in place for approved researchers. In all cases such access will be managed in accordance with our legal obligations, the standards set out in the Code of Practice for Official Statistics and our published procedures.

6.5.6 Any proposals for access to micro-data samples (anonymised data for individuals and households) will be developed in light of the disclosure control methods applied to the underlying data, access agreements and licensing issues.

6.6 Data Retention and Destruction

6.6.1 The integrity and security of information assets is a core principle underpinning all the work that we do. ONS has well established policies and procedures governing the retention and destruction of data. Full account will be taken of statutory requirements such as those set out in the Data Protection Act 1998, agreed Government standards and ONS's confidentiality and security policies.

Online census

6.6.2 In 2011, we scanned the paper questionnaires and created similar images for the online census returns, as well as processing the data to create a statistical database. The images were transferred to microfilm and will be released after 100 years for use by genealogists and family historians.

6.6.3 It is not possible at this stage to comment on the detailed methods that may be used to capture information from an online census in 2021. Although technological advances in data capture and retention may necessitate a change in approach from that adopted for the 2011 Census, we can anticipate that there will be an ongoing need to create and maintain a statistical database and to meet the needs of genealogists and family historians.

6.6.4 In accordance with standard practice we can anticipate that:

- data will be held securely and safely
- access to any census personal information will be limited to those who have an appropriate need, the required approval and security clearance
- published results will be produced from a database that does not contain identifiable individual information

Administrative and survey data

6.6.5 ONS will draw on its extensive experience in managing data from both administrative sources and surveys to ensure that any information collected and held to meet future user requirements for population and socio-demographic data will be managed in accordance with our statutory duties and Principle 8 in the Code of Practice for Official Statistics.

6.6.6 As far as data from administrative sources or systems are concerned ONS will comply with legal obligations and any specific terms and conditions set out in individual data access or service level agreements. At the same time any survey data will be managed in accordance with our data retention, preservation and archiving policy and take account of any specific obligations to survey respondents.

6.6.7 In all cases our work will be guided by the following core principles and standards:

- safeguarding confidentiality and keeping all the information that we use safe and secure
- retaining data only for as long as necessary to carry out the required statistical work
- ensuring that our information systems (e.g. facilities such as the SRE) comply with government security and technical standards
- complying with standards for the destruction of protectively marked information and the disposal of any media used for the storage or processing of protectively marked information (e.g. HMG IA Standard No. 5 Secure Sanitisation)

6.7 System De-commissioning

6.7.1 At this point it is too early to comment on any detailed arrangements that may be made to ensure that any systems no longer required by ONS are closed down appropriately and that steps are taken to evaluate and manage the risks associated with the disposal of any equipment. In particular, special attention will need to be given to the disposal or re-use of equipment or media to ensure that the confidentiality of any personal data we have accessed, collected or processed for statistical purposes is not compromised. In all cases full account will be taken of our legal obligations and ethical standards.

Online census

6.7.2 The temporary 2021 online census applications will be closed down when the data collection phase of the census operation has been completed. After the data has been transferred for further quality assurance all data held on such services will be 'wiped' in line with government requirements.

6.7.3 Similar protocols and procedures will apply to the systems established and used by any census suppliers for the 2021 online census. The need to comply with accepted government standards will be incorporated into all relevant contracts, monitored and enforced by accredited security experts.

Administrative and survey data

6.7.4 The risks associated with the decommissioning of any systems and disposal of any related equipment associated with the collection or use of administrative and survey data will be evaluated fully and managed with care. Government standards will be rigorously enforced in order to meet legal, contractual and ethical requirements, not least those set out in agreements with data suppliers and the commitments we make to survey respondents.

6.7.5 All infrastructure including IT equipment and any media holding protected or sensitive data no longer required by ONS will be decommissioned in line with government standards. Special account will be taken of the need to ensure that any personal data held on such equipment or systems is removed safely and securely.

7 Legal Compliance

7.1 The processes implemented by ONS to meet its statutory obligations to produce and publish official statistics that serve the public good[23] must be lawful. ONS must be satisfied that it can comply with all relevant duties and prohibitions relating to the processing and disclosure of personal information, whether collected directly from an online census or survey or indirectly from administrative sources. In particular, account must be taken of ONS-specific laws such as the Census Act 1920, data sharing and general privacy legislation most notably the Data Protection Act 1998 and the Human Rights Act 1998. Further details are set out below.

Online census

7.2 The authority to undertake a census in England and Wales is set out in primary legislation, that is, the Census Act 1920. The duty previously conferred on the Registrar General, by section 2 of the Census Act, to make all the necessary arrangements for the taking of a census, was transferred to the Statistics Board (now the UK Statistics Authority) by provisions in the Statistics and Registration Service Act 2007 [24].

7.3 The details or particulars to be stated in the returns are prescribed and set out in the Schedule to the Census Act 1920. They include:

- name, sex, age
- occupation, profession, trade or employment
- nationality, birthplace, race, language
- place of abode and character of dwelling
- condition as to marriage, relation to head of family, issue born in marriage, and
- any other matters relating to the social or civil condition of the population

7.4 Subsequently, the Census (Amendment) Act 2000 made provision for the collection of information on religion on a voluntary basis.

7.5 The Census Act includes provisions for secondary legislation to set out the detailed arrangements governing the conduct of each census. ONS is able to take a census only after Parliament has approved the relevant legislation.

7.6 There are three stages to the parliamentary process:

[23] s.7(1) Statistics and Registration Service Act 2007 refers to the need to promote and safeguard the production and publication of official statistics that serve the public good.

[24] Relevant details are set out in s.25 and Schedule 1 Statistics and Registration Service Act 2007.

(i) White Paper[25] - although this is not a legal requirement such a document is usually presented to Parliament in a written ministerial statement. The White Paper will outline proposals for a census including possible topics and questions for inclusion as well as any planned changes to the census operation and methods. For an online census in 2021 we can anticipate that this would include details relating to the completion of the required questionnaires, the use of administrative data as well as the associated security arrangements.

(ii) Census Order (Order in Council) - directs that a particular census shall be taken and states:

- the date of the census
- the area to be covered by the census
- the persons required to complete the census returns
- the persons required to be included in the returns, and
- the content of the questions to be answered

The Order must be approved by both Houses of Parliament and then 'made' by the Privy Council. In accordance with provisions in the Government in Wales Act 1998 the appropriate Welsh Minister must be consulted on the content of the Census Order.

(iii) Census Regulations - set out the procedures and practical arrangements for each census in England including, for example, the methods that would be applied for any online data collection in 2021 as well as the measures that would be taken to facilitate participation and safeguard confidentiality.

The Minister for the Cabinet Office is responsible for laying the Regulations which are subject to the negative resolution procedure of both Houses of Parliament[26].

The responsibility for making Census Regulations with respect to a census in Wales rests with Welsh ministers. Responsibility was transferred from the Chancellor of the Exchequer to the National Assembly for Wales in December 2006 by virtue of a Transfer of Functions Order (TFO) made under the provisions of the Government in Wales Act 1998. Separate Regulations for Wales would be laid before the National Assembly for Wales.

[25] White papers are documents produced by the Government setting out details of future policy on a particular subject prior to the introduction of legislation.

[26] Negative resolution - the Regulations become law without a debate or a vote but may be annulled by a resolution of either House of Parliament. Such instruments become law unless there is an objection from the House. The instrument is laid in draft and cannot be made if the draft is disapproved within 40 days.

7.7 Responsibility for censuses in Scotland and Northern Ireland lies with the National Records of Scotland (NRS) and the Northern Ireland Statistics and Research Agency (NISRA).

European Census Legislation

7.8 The census has been carried out since 1801 primarily to meet national needs. However, we can anticipate that European Union (EU) regulations similar to those put in place for 2011[27] will apply to the next census round in 2021.

7.9 The European Parliament and Council will expect all member states to provide specified statistical outputs based on a census (or comparable data sources). These outputs will be provided to Eurostat, the Statistical Office of the European Community, and will be used as the basis for comparisons between countries and regions to support specific policies and objectives (e.g. allocation of structural funds). ONS is responsible for bringing together the census results from Scotland, Northern Ireland, England and Wales and for the provision of harmonised UK outputs. Any information provided to Eurostat would be in the form of aggregate (i.e. non-disclosive) statistics. Special attention will need to be given to the availability, quality and comparability of UK outputs.

Administrative data

7.10 ONS can only make use of data collected and held by other public authorities where it is lawful. Provision is usually made in either primary or secondary legislation but in some cases common law powers may be applied. Details of the arrangements governing access to, and use of data, during the initial research phase are set out in Section 6.1 and Annex A.

7.11 Any administrative data that ONS obtains can only be used for statistical purposes and can only be shared with other statistical organisations such as NRS and NISRA where there is explicit legal authority for such onward disclosure. In all cases the disclosure would be subject to the same terms and conditions applied to ONS and the confidentiality provisions specified in the Statistics and Registration Service Act 2007[28].

Other Statutory Requirements

7.12 In addition to legislation governing specific statistical functions ONS must comply with all data protection and privacy legislation. Our obligations for both an online census and the use of administrative and survey data in relation to the Human

[27] Framework Regulation (EC) No 763/2008 of the European Parliament and Council of the EU and a series of implementing measures:
- Commission Regulation (EC) No 1201/2009;
- Commission Regulation (EU) No 519/2010;
- Commission Regulation (EU) No 1151/2010.

[28] s.39 Statistics and Registration Service Act 2007.

Rights Act 1998, the Data Protection Act 1998 and the Law of Confidence are considered below.

Human Rights Act 1998

7.13 The Human Rights Act 1998 codifies protections set out in the European Convention on Human Rights including those set out in Article 8 which relate to respect for private and family life[29]. Proposals for an online census in 2021, the increased use of administrative or survey data must be compatible with this Article, which states that:

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

2. 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.

7.14 As these are qualified rights a public authority may enquire into a person's private life where they have a legal authority to do so and where such an enquiry is necessary in a democratic society for one of the aims stated in the Article. This was tested in a court of law in 2002 when it was found that the census was compatible with Human Rights legislation.

7.15 **Online census** - the Census Act and the associated secondary legislation will provide the lawful authority for an online census in 2021. Furthermore, any 'interference' associated with such a proposal will be justified because the collection and processing of any population and socio-demographic data will be necessary for the production of statistics used by central and local government, businesses, voluntary, charitable and other organisations to promote economic well-being, protect health, safeguard community cohesion and the rights and freedoms of all.

7.16 **Administrative and survey data** - any 'interference' will be justified because the data collected and processed will, in all cases, be used to meet identified requirements and produce statistics to support the work of central and local government and other organisations (see above).

[29] s.1 and Schedule 1 Human Rights Act 1998.

Data Protection Act 1998 and other privacy legislation

7.17 The Data Protection Act 1998 governs the protection of personal data. Although it creates responsibilities for those who process, store or transmit such data there are exemptions for research, statistical or historical purposes specified in s.33 of the Act[30].

7.18 Any detailed proposals for an online census will need to take account of the data protection principles specified in Schedule 1 of the Act. Further details on these core principles and related conditions are set out in Annex C. Requirements to comply with these principles apply equally to an online census and the use of administrative and survey data.

7.19 **Principle 1:** Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

7.20 **Online census** - the relevant Schedule 2 condition is that the processing will be necessary for compliance with our legal obligations under the Census Act 1920 and any related secondary legislation. In the case of any sensitive personal data the Schedule 3 condition that would apply will be that the processing is necessary for the functions of the Crown, a Minister of the Crown or a government department.

7.21 **Administrative and survey data** - Schedule 2 conditions 5(c) and 5(d) would apply as the processing will be necessary for the exercise of functions of a government department and to enable ONS to carry out its duties "of promoting and safeguarding the production and publication of official statistics that serve the public good"[31]. Similarly, the processing of any sensitive personal data will be covered by the same Schedule 3 condition that would apply to an online census (that is the processing is necessary for the functions of the Crown, a Minister of the Crown, or a government department).

7.22 **Principle 2:** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

---

[30] s.33(1) - in all cases any such processing must comply with the following conditions:
(a) the data are not processed to support measures or decisions with respect to particular individuals, and
(b) the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

[31] s.7(1) Statistics and Registration Service Act 2007.

7.23 **Online census** - the questions to be asked will be specified in the Census Order and designed to meet specific user requirements. The data may be used only for statistical purposes.

7.24 Any data processed by ONS or any third parties will be managed in accordance with arrangements set out in the Census Order and Census Regulations, the Statistics and Registration Service Act 2007 and the Code of Practice for Official Statistics. Moreover, in accordance with provisions in section 33 of the Data Protection Act, further processing of personal data for statistical purposes is not incompatible with the purposes for which they were obtained.

7.25 **Administrative and survey data** - the information required will be designed to meet users' needs and to enable ONS to carry out its specified functions. Any further processing will be managed in accordance with requirements in the Statistics and Registration Service Act, the terms and conditions agreed with individual data suppliers, obligations in the Code of Practice for Official Statistics and our Survey Charter and provisions in section 33 of the Data Protection Act (see paragraph 7.24 above).

7.26 **Principle 3:** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

7.27 **Online census** - ONS will undertake a programme of consultation, question development and testing to ensure that the information it collects will meet specified statistical needs. In all cases the information must be fully justified. The details of the questions to be asked will be set out in the Census Order which must be approved by Parliament.

7.28 **Administrative and survey data** - requirements for information will be carefully assessed and designed to meet identified needs. Access to data from administrative sources must be justified via the preparation of business cases or other procedures specified by individual data owners including the preparation of PIAs. In all cases access will be authorised by relevant legislation or common law powers (see Section 6.1 and Annex A for further details). In addition ONS will be bound by the principles set out in the Code of Practice for Official Statistics and our Survey Charter.

7.29 **Principle 4:** Personal data shall be accurate and, where necessary, kept up to date.

7.30 **Online census and administrative and survey data** - ONS will make every effort to ensure that the data collected and used to produce census outputs is as accurate as possible. It is not necessary to keep census information up-to-date as it relates to a snapshot in time.

7.31 **Principle 5:** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7.32 **Online census and administrative and survey data** - in accordance with provisions in s.33 of the Data Protection Act information kept and used for purely statistical purposes may be kept indefinitely[32].

7.33 ONS will make appropriate arrangements to ensure that any personal data it uses to produce statistical outputs is kept safe and secure and is managed in accordance with any specific terms and conditions agreed with individual data suppliers as well as standards set out in the Code of Practice for Official Statistics and our Survey Charter.

7.34 **Principle 6:** Personal data shall be processed in accordance with the rights of data subjects under this Act.

7.35 **Online census and administrative and survey data** - as the information will be used for statistical purposes data subjects have no right to make a subject access request.

7.36 Processes are in place to ensure that any questions or objections, including those associated with s.10, s11, s.12 or s.14 Data Protection Act notices, are dealt with by the ONS Data Protection Officer.

7.37 **Principle 7:** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7.38 **Online census and administrative and survey data** - as previously indicated in other parts of this document (e.g. Sections 6.1 to 6.4) appropriate technical and other measures will be taken to ensure that there is no unauthorised or unlawful processing, accidental loss, damage or destruction of any personal data collected as part of an online census or the use of data from administrative and survey sources.

7.39 **Principle 8:** Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.40 **Online census and administrative and survey data** - there are no plans to transfer personal data outside of the European Economic Area.

[32] Section 33 of the Data Protection Act 1998 states that personal data processed for research purposes, including statistical or historical purposes, may be kept indefinitely.

Law of Confidence

7.41 A duty of confidence arises when confidential information comes to the knowledge of a person in circumstances where it would be unfair if it were disclosed to others. Any action for breach of confidence would need to prove that the information:

- has the necessary degree or quality of confidentiality
- has been provided in circumstances and with the expectation that it would be treated in confidence, and
- has been used or disclosed for an unauthorised purpose and with an associated risk of damage

7.42 Any personal information provided to ONS may be used only for statistical purposes. Furthermore, no decisions or actions would be taken which would be detrimental to an individual.

7.43 This initial review has demonstrated that proposals for an online census in 2021 or for the use of administrative and survey data will be lawful and will be carried out in accordance with our statutory obligations to protect the privacy of any personal data we may be required to access, collect, process and use for work associated with the development, derivation and publication of population statistics.

8 Conclusion

8.1 This initial PIA covers work being taken forward by the Beyond 2011 Programme. It underlines ONS's commitment to uphold the highest standards of data integrity and confidentiality as well as the importance that we place on maintaining public trust and our excellent reputation.

8.2 Over the past three years we have undertaken a comprehensive programme of consultation and stakeholder engagement. This has underlined the ongoing need for consistent and comparable information about the population and housing including details on households and families as well as the special importance of providing statistics for small areas and small sub-groups of the population. Our work has shown that the census continues to be highly valued by government, local authorities, other public and voluntary organisations, businesses, academic and research institutions, commentators, citizens, genealogists and family historians. Despite the increasing pace of societal change, information from the census still underpins the allocation of billions of pounds of public money, supports decision making, policy formation, service planning and delivery, research and outcome monitoring.

8.3 The report has outlined the processes and procedures that have been put in place by ONS and will provide the basis for subsequent research work. Using the criteria in our assessment framework has enabled us to ensure that appropriate measures have been taken to manage and mitigate privacy risks associated with:

- **accessing data from administrative sources** - not only must ONS fully justify its statistical requirements but also comply with relevant legislation (e.g. the Data Protection Act 1998), the Government's Security Policy Framework and relevant technical standards
- **collecting data** - full account has been, or will be, given to our statistical obligations and ethical standards(e.g. the 1920 Census Act and Code of Practice for Official Statistics), relevant security standards and technical measures in order to safeguard confidentiality, counteract threats from hacking or other malicious actions
- **processing data** - administrative data used for research purposes are, or will be, pseudonymised. Work will continue to be carried out in the SRE which has been independently tested and accredited
- **preparing and publishing statistics** - all outputs disseminated by ONS must be non-disclosive
- **archiving or destroying data** - arrangements are governed by statutory obligations such as those in the Data Protection Act 1998, government standards, ONS's confidentiality and security policies as well as specific conditions specified by data owners in data access agreements

8.4 Our programme of consultation and stakeholder engagement, research on public acceptability, oversight by data suppliers, security and technical experts testifies to the careful and thorough approach that has been taken. While we are confident that the systems and processes we have put in place are robust, we recognise the need for constant vigilance and regular reviews to ensure that proper account is taken of changing research plans and priorities. ONS will build on the work that has been done to ensure that future design and operational decisions will comply with statutory requirements and ethical standards as well as relevant technical, security and data handling standards.

9 Next Steps

9.1 In accordance with guidance issued by the Information Commissioner's Office this PIA will be viewed as a living document. It will be reviewed and amended as work proceeds and more detailed decisions are made. Information provided by the public, whether directly or indirectly, will be well protected in accordance with statutory requirements, government security standards and information assurance procedures. At this early stage it is anticipated that special attention will need to be given to the following:

- engagement with stakeholders, users and others with an interest in the future provision of population statistics in England and Wales to explain the issues and implications associated with the National Statistician's recommendation and our ongoing programme of work
- continuing research to improve our understanding of public attitudes to the census and data sharing
- developing and testing questions to meet identified needs
- detailed design and operational decisions
- plans to integrate data from surveys and administrative sources
- any changes to the Government's Security Policy Framework, technical or other relevant standards
- any legislative developments

9.2 ONS is committed to safeguarding the confidentiality of all the information that it collects and processes in order to produce and publish statistics that serve the public good. We shall continue to consult widely, seek advice from relevant experts and provide updates on our progress and plans. The methods used to protect personal information gathered for the 2021 census or related operations will be independently reviewed and the results published on the ONS website as they were in both 2001 and 2011.

9.3 The public can be assured that any intrusion on privacy will be justified and that ONS will be open and transparent about the processes and procedures that it will put in place to safeguard the security and confidentiality of any information that it collects or processes to meet future requirements for population statistics.

Annex A: Legal Authority for Access to Data

Details of the arrangements that have been made to authorise access to, and use of, data for the research stage of the Beyond 2011 Programme are outlined below.

2011 Census and Census Coverage Survey - Census Act 1920, Census Order and Census Regulations provide the authority for ONS to take a census and obtain statistical information on the population and cover all relevant aspects of the census operation. The Statistics and Registration Service Act 2007 enables ONS to make use of this information for other research and statistical purposes.[33]

Statistics and Registration Service Act 2007 - includes provisions to enable the sharing of personal information for statistical purposes. The Act allows ministers to:

- make regulations to remove barriers to data sharing between public authorities and the UKSA; and
- provide public bodies with a power to share data if none exists.

Before any regulations can come into force in England and Wales, a draft must be laid before Parliament and be approved by affirmative resolution. In all cases the Minister for the Cabinet Office and the minister responsible for the public authority involved in the data share must be satisfied that the data sharing is necessary and is in the public interest.

The data sharing provisions have been used on four occasions to secure access to a sub-set of information from the following sources:-

School Census in England - covered by the Disclosure of Pupil Information (England) Regulations 2009.

School Census in Wales - covered by the Disclosure of Pupil Information by Welsh Ministers Regulations 2011.

Student Record - covered by the Disclosure of Higher Education Student Information Regulations 2009.

Customer Information System - covered by the Disclosure of Social Security and Revenue Information Regulations 2012.

In addition, the Statistics and Registration Service Act 2007 makes provision for the disclosure and use of patient registration data and information on births and deaths.

Patient Register - s.43 and s.44 authorise the disclosure of patient registration information in England and Wales and its use for the production of population statistics.

[33] s.38(1) Statistics and Registration Service Act 2007 states that " Any information obtained by the Board in relation to the exercise of any of its functions may be used by it in relation to the exercise of any of its other functions".

Births and Deaths - s.42 authorises the Registrar General for England and Wales to disclose information on births and deaths.

Lifetime Labour Market Database (1% sample) - disclosure of a sub-set of data authorised by s.3 Social Security Act 1998 and s.22 Statistics and Registration Service Act 2007.

Electoral Registers - access for statistical purposes authorised by Regulation 99 The Representation of the People (England and Wales) (Amendment) Regulations 2002.

e-Borders/Border Systems Programme - data on passenger transfers authorised in accordance with common law powers and in compliance with obligations under the Data Protection Act 1998.

AddressBase - authorised by the Public Sector Mapping Agreement .

Annex B: Specification of Cryptographic Functions

Research into options for the production of population and small area socio-demographic statistics requires the linkage and analysis of large amounts of individual-level administrative data from sources such as the NHS Patient Register and the Customer Information System (see Annex A for further details). In order to comply with legal, regulatory and inter-departmental security requirements as well as our obligations to safeguard confidentiality, a strong cryptographic hash[34] is used to ensure uniquely-identifying variables within source data are not identifiable to those undertaking the statistical research. Full account has been taken of guidance provided by the Information Commissioner's Office[35]. We have intentionally selected proven industry standards to allow public scrutiny of our approach.

The approach adopted is focused on protecting individual-level personally-identifiable information. Summary details relating to the two key stages involved are outlined below.

Stage 1 Per-field Key Generation - for each field that needs to be hashed within source datasets, and for each derived 'matchkey', a unique random key is generated and held securely for as long as required. One unique random key is generated per field that needs to be matched, with each key being used for similar fields across different datasets - e.g. a 'Postcode key', a 'Forename Key', ' A Matchkey 1 Key', etc.

Ideally, these keys should be truly random, or at least generated using a Cryptographically Strong Pseudorandom Number Generator (CSPRNG). The SRE takes the CSPRNG approach. The length of the keys are 1024 bits (128 bytes, or 256 hexadecimal digits), as this is the optimum key size for the Hash-based Message Authentication Code (HMAC) HMAC-SHA512 algorithm used in Stage 2.

Stage 2 Hashing Operation - every time a source dataset is imported, each identifying variable and 'matchkey' is hashed using a key-based hashing algorithm which combines the field content with the unique key from Stage 1 to produce a final consistent, irreversible value based on the original field input.

The hashing algorithm selected for SRE purposes is the HMAC, using SHA-512 as the hashing algorithm (HMAC-SHA512). The final output from this process is always a 512-bit (64-byte) hash value, which is represented as a hexadecimal string (128 characters). Since the use of multiple 128-character strings in operation can lead to storage and performance issues, truncation of this value has been used to reduce overhead - the first 128 bits (16 bytes, 32 hex digits) of the hash value are used in the

[34] Hashing is a one-way, irreversible process, as opposed to encryption which is designed to be reversible.

[35] 'Anonymisation: managing data protection risk code of practice', Information Commissioner's Office, November 2012.

final datasets. This level of truncation does not introduce a significant risk of collision[36], whereas further truncation might.

The processes and procedures we have adopted to safeguard the confidentiality of all the data that we use have been independently reviewed by leading experts.

Further details are available in the paper 'Safeguarding Data for Research: Our Policy'.

Any proposals to implement an approach based on the use of administrative and survey data would need to consider the feasibility and acceptability of current methods.

[36] 'Collision' is where multiple different raw values produce an identical hash, resulting in a reduction in statistical quality and confidence.

Annex C: Data Protection Act 1998 - Data Protection Principles and Conditions

Schedules 1, 2 and 3 of the Data Protection Act 1998 set out the principles and conditions relevant to the processing of personal data and sensitive personal data. Further details are summarised below.

Schedule 1: The Data Protection Principles

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 2: Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data

1 The data subject has given his consent to the processing.

2 The processing is necessary –

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary –

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3: Conditions Relevant for Purposes of the First Principle: Processing of Sensitive Personal Data

1 The data subject has given his explicit consent to the processing of the personal data.

2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order –

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary –

(a) in order to protect the vital interests of the data subject or another person, in a case where –

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing –

(a) is carried out in the course of its legitimate activities by any body or association which –

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing –

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1) The processing is necessary –

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order –

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A (1) The processing –

(a) is either –

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8. (1) The processing is necessary for medical purposes or is undertaken by –

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1)The processing –

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purpose of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.