UK Statistics Authority

Draft Research Code of Practice and Draft Accreditation Criteria

Presented to Parliament pursuant to section 70(9) of the Digital Economy Act 2017 for approval by resolution of each House

May 2018

Contents

Part 1: Draft Code of Practice[1]

About the Code of Practice and Accreditation Criteria

1.1 Through Chapter 5 of Part 5 of the Digital Economy Act 2017 ('the Act') the UK Parliament has enacted legislation, applicable across the UK, that facilitates the linking and sharing of datasets held by public authorities (as defined in the Act) for research purposes. The provisions aim to broaden the capacity of research to deliver a number of direct and indirect public benefits, including the production of valuable new research insights about UK society and the economy.

1.2 The power set out in Chapter 5 ('the Research power') broadly enables information held by one public authority to be disclosed to another person for the purposes of research being, or to be, carried out. It also sets out a process for 'de-identifying' personal information to be shared under the power. To provide clarity and transparency about how the power will operate, the Act requires the UK Statistics Authority (hereafter 'the Authority')[2] to issue a Code of Practice concerning the disclosure, processing, holding or use of personal information under this gateway. The Authority must consult as set out in the Act before issuing or reissuing this code, and must lay the code before the UK Parliament and the devolved legislatures in Scotland, Wales and Northern Ireland.

1.3 The Act requires three groups of people to have regard to the principles set out in this Code:

- Data-holding public authorities[3] when disclosing personal information or processing for subsequent research purposes under the Research power;
- Those accredited for the purposes of processing this data, whether that processing be concerned principally with the linkage or de-identification of data, or the storage and provision of secure access to the de-identified data; and,
- Individuals to whom de-identified data is made available for research.

1.4 The Act further requires that all persons involved in the processing or use of information under this gateway for disclosing information under this power, secure accreditation appropriate to the functions they seek to exercise under the Act. The Act identifies the Authority as the body responsible for overseeing this accreditation process and requires the Authority to publish a set of criteria that individuals, organisations and research projects must meet before being accredited for any of the functions set out in the Act. Details of the criteria for accreditation are set out in Part 2 of this document.

1.5 In drawing up the code and the accreditation criteria, the Authority has had regard to, inter alia, the:

- Information Commissioner's Data Sharing code of practice (2011)[4]

[1] This Part comprises the Code of Practice required under section 70(1) of the Digital Economy Act 2017
[2] These legal obligations rest in "the Statistics Board", that is, in the Board of the UK Statistics Authority. Under the authority of the Board, the work of the UK Statistics Authority and its executive office, the Office for National Statistics, gives effect to the duties enshrined in the Digital Economy Act. Within this document "the Authority" is used to reflect this arrangement.
[3] The Act provides that, insofar as a public authority has functions relating to the provision of health services or adult social care, section 64 of the Act does not authorise the disclosure of information that public authority holds in connection with those functions.
[4] As altered or replaced from time to time.

- Information Commissioner's Anonymisation: Managing Data Protection Risk Code of Practice (2012)
- Information Commissioner's Conducting Privacy Impact Assessments Code of Practice (2014)
- Information Commissioner's Privacy Notices, Transparency and Control Code of Practice (2016)
- Statistics and Registration Service Act 2007
- Code of Practice for Official Statistics
- The data protection legislation[5]
- The Ethical Principles of the National Statistician's Data Ethics Advisory Committee
- Report of the Administrative Data Taskforce (2012)
- Cabinet Office Open Data White Paper (2012)

Understanding the power

2.1 The Act helps to position the UK at the forefront of the international research landscape and supports a number of direct public benefits while protecting the confidentiality of personal information. The power will help achieve this by:

- increasing the availability of varied and high-quality data for researchers within and outside government, which will help drive improvements in the evidence base available to policy and other key decision-makers;
- facilitating the linkage of datasets held by two or more public authorities in controlled environments, which offers increased opportunities for new insights into the social and economic challenges that citizens and businesses face;
- helping researchers and policy-makers build a better understanding of how people live their lives, their patterns of need and use of different services and the resultant outcomes, to support the design and delivery of more effective and efficient public services.

2.2 The Act will help to provide certainty and clarity for public authorities and researchers that data can be disclosed for research purposes and the conditions under which that data can be disclosed. This will help to reduce the delays and inconsistent approach to releasing publicly-held data for research purposes, helping to ensure that the economic and social benefits associated with research are more easily realised.

2.3 The Research power in the Act is a permissive gateway to enable public authorities to make information available to researchers for the purpose of research in the public interest, provided a number of conditions are met. There are requirement built into the Research power requiring certain parties involved in the disclosure of this information to be accredited, following a process set out in section 71 of the Act. Before personal information can be shared for research purposes, it must be 'processed' either by an accredited third party or the data-holding public authority itself (in both cases referred to

[5] "The data protection legislation" means the full, applicable data protection framework as set out in the Data Protection Act 2018. This encompasses general processing (including the General Data Protection Regulation and the applied GDPR), law enforcement processing, and intelligence services processing. References to "the Data Protection Act 1998" in the Digital Economy Act 2017 are amended to "the data protection legislation" by the Data Protection Act 2018.

as 'the processor'). In addition to processing data so that personal information is de-identified, a processor will need to have procedures in place for the linking, storing and curating of data, and other related procedures as appropriate. When the information has been processed, it can be disclosed to an accredited researcher in a secure environment. The accredited processor must take reasonable steps to ensure that any data (or analysis based on the data) that are retained by the researcher, or are published, undergo a disclosure control process to minimise the risk of the data subjects being re-identified or other misuses of the data.

2.4 To ensure data are processed and made available to accredited researchers in a safe and secure way (and in line with the requirements of the data protection legislation), the Act sets out six conditions under which information can be disclosed under the Research power:

- Data must be de-identified before they can be made available so that the data do not directly identify individuals and are not reasonably likely to lead to an individual's identity being ascertained (whether on its own or taken together with other information);
- The parties involved in processing and providing access to the data must take reasonable steps (meaning implementing and maintaining appropriate safeguards) to minimise the possibility that identifying data might be accidentally or intentionally disclosed;
- Once data are suitably processed, the data can be made available to the researcher for the purposes of the accredited research;
- The research for which the de-identified data are being made available is in the public interest and has been assessed as such through an accreditation process;
- The researcher(s) and all persons involved in processing the data are accredited for these functions; and,
- Public authorities disclosing data to trusted third parties for processing and making de-identified data available for research purposes, and trusted third parties involved in processing information for the same purpose, have regard to this code of practice.

2.5 This Code contains seven principles of data sharing for research purposes, intended to collectively ensure that the processing and provision of personal information under the Act is ethical and legal, and done in a way that ensures information that relates to an individual (whether or not this information identifies the individual) is appropriately protected. All parties who disclose, process, or use data under the Research power are expected to adhere to these principles in performing their function under the Research power. Although not binding for disclosures of non-personal information under this gateway, the principles set out below should be considered as good practice for all those involved in non-personal information disclosures for research purposes.

Principles governing the disclosure of data

Principle 1: Confidentiality

3.1 All persons disclosing, making data available, processing or using data under the provisions set out in the Act must ensure they do so in a way that does all that is

necessary to minimise the risk of compromising the confidentiality of personal information. Appropriate safeguards must be established and maintained at all stages of, and by all persons involved in, the handling of data and their use for research purposes under this gateway, proportionately to the sensitivity of that data. All persons using the Research power must maintain the integrity of these safeguards by proactively identifying and assessing the privacy and security risks, and by regularly reviewing safeguards and security solutions to ensure they continue to meet the challenges posed by evolving technologies.

Principle 2: Transparency

4.1 All parties using the Research power should adopt a commitment to transparency by default in order to maximise the potential public value of research facilitated by access to data held by public authorities. Ensuring information sharing practices are fair and transparent is also necessary to ensure compliance with the GDPR's 'lawfulness, fairness and transparency' principle (see Article 5(1)(a)).[6] Researchers should routinely engage core stakeholders on the findings of the research drawn from these data, and ensure that research findings are made openly available to the public. Data-supplying public authorities and processors should publish information about the data they are disclosing, the rationale and purpose of doing so, and any restrictions and safeguards associated with the processing and use of those data. Decisions concerning whether or not to publish such information may be informed by security or other considerations where the risks of publishing such information would outweigh the potential public benefits. In its accreditation capacity, the Authority may also choose to publish details on data requests and accreditation applications and outcomes, including the outcome of any appeals process.

Principle 3: Ethics and the law

5.1 Data can only be disclosed to processors (for the purpose of subsequently making de-identified data available to researchers) where expressly permitted, and must comply with the six conditions set out in the Act. In disclosing data under the Research power, data holders, processors and researchers must also meet all legal obligations arising from the data protection legislation,[7] and other applicable legislation; and are expected to have regard to best practice on privacy impact assessments and privacy notices, as set out in the Information Commissioner's Conducting Privacy Impact Assessments Code of Practice and Privacy Notices, Transparency and Control Code of Practice (which provides guidance on the contents of these notices, as well as where and when to make them publicly available). The data protection legislation requires 'data protection impact assessments' to be conducted prior to the processing when the processing is likely to result in a high risk to the rights and freedoms of individuals. The data protection legislation also requires privacy notices to contain more detailed and specific information than under the Data Protection Act 1998.

5.2 All parties involved in the disclosure, processing or use of data through the Research power must observe the ethical standards appropriate to the nature of the research, ensuring that the unique ethical challenges presented by using data collected for

[6] The 'accountability' principle in Article 5(2) of the GDPR makes data controllers responsible for demonstrating that the 'lawfulness, fairness and transparency' principle, together with the other principles set out in article 591), have been complied with.

[7] This will include compliance with Article 28 GDPR, which sets out information that will need to be contained in the relevant documentation (including accreditation documentation) underpinning any data sharing arrangement under these powers.

operational purposes are accounted for and addressed in the discharging of each of the functions described within the Act. For example, the Ethical Principles of the National Statistician's Data Ethics Advisory Committee involve ensuring the appropriate consideration of issues of privacy, identifying and minimising the risks of re-identification, and considering risks appropriate to the type, scale and sensitivity of the data being disclosed. It may also require reflecting on the risks and limits of new technologies, oversight practices and adherence to recognised methodological and quality standards, legal obligations and public acceptability.

Principle 4: Public interest

6.1 Data obtained under the Research power must only be disclosed, processed and used for the purpose of supporting research in the public interest. Research in the public interest is research whose primary purpose is, for example, to:

- provide an evidence base for public policy decision-making;
- provide an evidence base for public service delivery;
- provide an evidence base for decisions which are likely to significantly benefit the economy, society or quality of life of people in the UK, UK nationals or people born in the UK now living abroad;
- replicate, validate, challenge or review existing research and proposed research publications, including official statistics;
- significantly extend understanding of social or economic trends or events by improving knowledge or challenging widely accepted analyses; and/or,
- improve the quality, coverage or presentation of existing research, including official or National Statistics.

6.2 The Authority has set out further information concerning the criteria for determining whether research is in the public interest in the criteria for the accreditation of research projects (see Part 2: Accreditation Criteria).

Principle 5: Proportionality

7.1 Data must be disclosed or made available in a way that ensures the burdens and costs of doing so are proportionate to the anticipated benefits of the proposed research, regardless of who accrues the burden and costs. A researcher should ensure that in seeking to secure access to data held by public authorities he or she has assessed, insofar as he or she is able, suitable, less burdensome alternatives and is satisfied that no reasonable alternatives exist or that the financial or quality costs of securing data from other sources would be prohibitive. Equally, data-holding public authorities are required to provide data as efficiently as possible, and to ensure that any cost recovery charges are proportionate to work undertaken specifically for the purpose of releasing data for specified research projects.

Principle 6: Accreditation

8.1 All accredited persons and the research project itself must remain accredited for the duration of the project and at all times when processing, accessing or using the data, and must therefore observe the requirements for the maintenance of accreditation (such as training obligations). Data holders and accredited processors are also required to ensure that where they disclose or make data available to other processors or

researchers it is done for the specific purposes for which they have been accredited and only to a person that is accredited for the function they are fulfilling.

8.2 The Authority will ensure that it exercises its accreditation function in a way that is free from the influence of organisational, political or personal interests, and that the accreditation of applicants (or those whose accreditation is suspended or removed) have recourse to appropriate appeals mechanisms.

Principle 7: Retention and onward disclosure

9.1 Third party data processors (i.e. those who are accredited for the purposes of de-identifying personal information that are not the data-holding public authority itself) can only retain pre-processed, identified data for a limited time. The Authority will define this period as part of the accreditation process, subject to the consent of the relevant data-holding public authority, and in accordance with the nature of the data, good practice guidelines and any other relevant considerations. Data processors will be able to apply to the Authority for an extension of this period where there is a clear research rationale for doing so (such as in the case of longitudinal studies), subject to the consent of the relevant data-holding public authority.

9.2 Processors who store the de-identified data may make that de-identified data available to other researchers and for other research projects where all of the following criteria are met:

- where the data has been processed by a third-party data processor, the data-holding public authority has agreed to let that processor make the de-identified data available to additional individuals and/or for additional research projects;
- the processor remains fully accredited for its disclosure function; and,
- the researcher and the research projects are fully accredited for the use of these data.

9.3 Data processors must take reasonable steps that any data released to, and subsequently retained by, researchers for further analysis or publication undergoes a process of disclosure control to minimise the risk of its re-identification or other misuse of the data. In line with the requirements set out under the principles above, data should never be disclosed, made available in de-identified form or passed to any parties who are not suitably accredited under these powers.

Part 2: Draft Accreditation Criteria

10.1 The Digital Economy Act 2017 ('the Act') permits the disclosure of data held by public authorities for the purpose of conducting research in the public interest under the Research power in Chapter 5 of Part 5 of the Act ('the Research power'). This disclosure is conditional on the persons involved, and the research being carried out, being accredited by the UK Statistics Authority ('the Authority'). The Act requires[8] the Authority to establish and publish:

- conditions to be met by a person for accreditation under the Act;
- conditions to be met by research for accreditation under the Act; and,
- grounds for the withdrawal of accreditation under the Act from a person or from research.

10.2 This document sets out those conditions and grounds.

Section A: Accreditation of processors

11.1 The use of the Research power is conditional on the data being processed by an accredited processor. A processor must also be accredited for the functions of:

- linking, matching, curating and de-identifying of data; and/or
- storing and provision of access to de-identified data.

11.2 Any person(s) involved in the preparation, storing and provision of access to de-identified data must be accredited for the appropriate function. Accreditation documents will clearly state which of these functions the processor has been accredited for. The UK Statistics Authority will also publish details of accredited processors, along with details of which function(s) the accreditation covers. In some cases, the processor could be the public authority whose data has been requested if they have the necessary expertise. Public authorities undertaking any aspect of the processing of their own data for accredited research purposes – or indeed, linking and matching their data to that held by another public authority – must be appropriately accredited for the processing function they are performing. This will maintain standards of consistency throughout the accreditation process. If the researcher or any of the persons involved in processing the data do not, in the view of the Authority, act in a way that means they should remain accredited, the Authority may decide to withdraw their accreditation (see paragraph 22.1 below).

11.3 The Act introduces new criminal offences where personal information is received under the Research power and disclosed in breach of sections 66, 67, 68 or 69 of the Act.[9]

11.4 By default, an accredited processor will retain accredited status for up to five years with periodic reassessments, for as long as they continue to meet the conditions for accreditation set out below. After this time an accredited processor will need to apply for a renewal of its accredited status. From time to time emerging data threats and challenges may make it necessary to change the conditions required for accreditation as

[8] Section 71(2)(a), (b) and (c) of the Digital Economy Act 2017.
[9] See section 66(2), (5), (10), (11) and (12), section 67(2), (5) and (8), section 68(2),(5) and (8) and section 69(2), (5) and (8) of the Digital Economy Act 2017

a processor. In such circumstances the Authority may decide to provide notice of its intention to suspend and reassess the accreditation status of processors.

Conditions for accreditation of processors

12.1 To secure accreditation, processors (individuals involved in processing and the organisations to which they belong) must meet the following conditions:

The processor is a fit and proper person to perform the functions of a processor

13.1 Under section 71(3) of the Act, a person must be a fit and proper person to be involved in processing before the Authority will accredit them as a processor. In assessing this, the Authority will expect an applicant to provide appropriate evidence to confirm they have sufficient skills, experience, technical infrastructure and policies in place to demonstrate they are a fit and proper person. They will also need to demonstrate insofar as possible a record of appropriate compliance with UK laws, in particular laws relevant to processing activities and the use of data.

13.2 The Authority's assessment of skills, experience and compliance with relevant UK legislation will extend to the staff of the processor that would be involved in the proposed processing activities. When applying for accreditation as a processor, an applicant must advise the Authority of any matters that might affect the Authority's assessment of whether the person is a fit and proper person to be involved in processing under the Act, and provide evidence relating to these.

The processor must act under the territorial jurisdiction of the UK and comply with UK laws

14.1 Processors must be legally accountable for the work they carry out and must comply with UK law, whether enacted by the UK Parliament or, where processing is taking place within the jurisdiction of a devolved administration, by the appropriate devolved legislature. Processors must, in particular, ensure they comply with the legal requirements set out in the Act, the data protection legislation, the Human Rights Act 1998, and relevant provisions under the Investigatory Powers Act 2016 (including, until that Act comes fully into force, the equivalent provisions of the Regulation of Investigatory Powers Act 2000). Compliance may be assessed by an audit and is a central condition for the maintenance of a processor's accredited status.

The processor must meet appropriate cross-government standards for the secure holding of sensitive data

15.1 The UK Government maintains a security control framework setting out the physical, personnel and information security protocols required for the handling of all data assets collected, held and processed by government departments.[10] These protocols vary according to the way the data is classified in accordance with the sensitivity of the data and the risks associated with potential breaches. To protect the confidentiality of potentially sensitive data, any processor seeking accreditation under this gateway must provide evidence of meeting the current security controls

[10] https://www.gov.uk/government/collections/government-security
https://www.ncsc.gov.uk/guidance
https://www.cpni.gov.uk/advice

commensurate with the sensitivity of the data the processor will be handling. Where the processor wishes to process data under this gateway with a higher degree of sensitivity than that for which it has been accredited, it must inform the Authority and provide evidence it meets the additional security requirements.

The processor must have appropriate skills and experience

16.1 The processor must ensure that its staff have the necessary skills and experience to undertake the work required to the standards required, as appropriate for the processing function for which accreditation is sought. Staff involved in the preparation of data must have received training and be able to demonstrate their understanding of the linking, matching, and de-identification of data in a safe way; those involved in the provision of data must be able to demonstrate their experience and capacity to store and make de-identified data available safely. Individuals responsible for any aspect of the processing of data should also have security clearance appropriate to the nature of the data they are handling.

16.2 For auditing purposes the processor must agree to maintain a list of all those individuals who meet these requirements. The processor should also ensure that individuals are only involved in aspects of the processing for which they are suitably experienced and trained and that only suitably experienced and trained individuals have access to data provided by the public authority. All individuals involved in any aspect of the processing must sign a declaration confirming they have understood their responsibilities and will abide by the conditions imposed on them, including protecting the confidentiality of information they access under the legislation.

The processor must make use of appropriate technical infrastructure

17.1 The processor must use suitable data infrastructures to enable it to securely link, match, de-identify data, store and make de-identified data available, as appropriate for the specific function(s) the processor is fulfilling.

The processor must agree to publish and maintain appropriate data policies

18.1 At the point of application the processor must present, and maintain for as long as they wish to remain accredited, a set of detailed documents that demonstrate, to the Authority's satisfaction, that the processor will meet the requirements for handling, storing, protecting and destroying data it processes for research under the power. Specifically:

- A Secure Environments policy that ensures that the physical environment and processes meet the requirements to hold sensitive data. For processors seeking accreditation for the provision of data these policies must cover the operation of the secure data access facility where researchers can access data. Secure data processing facilities must be suitably accredited in line with cross-government security standards;
- A Major Incident protocol related to data security and privacy breaches;
- A De-Identifying Data policy;
- A Data Retention and Destruction policy; and
- A Data Confidentiality Breaches policy.

18.2 The processor must ensure that any data processing agreements are in place for any data it receives from public authorities before it processes that data. Whether or not an agreement is necessary will be determined on a case-by-case basis in discussion with the relevant data-holding public authority. The processor must also agree to abide by any additional policies and procedures the Authority has developed in its accreditation capacity. The Authority will provide appropriate notice where it intends to introduce new policy or procedural requirements.

The processor must agree to its inclusion on a public register

19.1 The Authority is required to maintain a public register of accredited persons. Any persons seeking accreditation for processing under this power must therefore agree to their inclusion on this register, unless there are exceptional reasons not to do so.

The processor must consent to being audited

20.1 In order to discharge its duty of oversight and ensure processors continue to meet relevant requirements, the Authority may, from time to time, decide to undertake an audit of accredited processors. Processors must consent to be audited during their accreditation application, and must fully comply with any audit that takes place in order to maintain their accredited status. The outcome of the audit will be communicated to the processor.

The processor must have regard to the Code of Practice

21.1 The processor must have regard to the Code of Practice and its principles when fulfilling any of its processing functions. Having appropriate regard to the Code is a central condition for the maintenance of a processor's accredited status and may be assessed by an audit.

Withdrawal of accreditation

22.1 Accreditation may be suspended or withdrawn from a processor accredited for the preparation or provision of data for one or more of the following reasons, where the processor:

- no longer meets any of the accreditation requirements;
- fails to have regard to the Code of Practice governing data sharing for research purposes;
- has breached the data protection legislation, as defined above, or other relevant legislation;
- has been convicted of relevant offences under the Act, the data protection legislation, as defined above, or other relevant legislation;
- has had any penalties imposed on it by the Information Commissioner's Office relating to processing under the data protection legislation, as defined above;
- has refused to provide or withdrawn the processing service for which it has been accredited;
- has brought the accreditation scheme into disrepute;
- refuses to be audited, or obstructs the auditing process; and/or,
- charges fees for processing, other than those ordinarily permitted for cost-recovery purposes.

Other considerations

23.1 The Authority will provide further guidance on the procedures and processes governing the accreditation of processors for the purpose of preparing or providing access to data under the Act. A processor who is refused accreditation, or who has their accreditation suspended or removed will have a right to appeal to the UK Statistics Authority as the accrediting body.

Section B: Accreditation of researchers and peer reviewers

24.1 Researchers undertaking research using data provided under the Research power must secure accreditation by meeting the conditions below. These conditions also apply equally to individuals seeking access to the data held by the processor for the purpose of reviewing that research prior to the publication of research outputs (peer reviewers).

Conditions for accreditation of researchers and peer reviewers

The researcher / peer reviewer must provide evidence of suitable research qualifications and/or experience

25.1 To demonstrate they have suitable research qualifications and/or experience, an individual must either:

- have an undergraduate degree (or higher) including a significant proportion of mathematics or statistics; or,
- be able to demonstrate at least 3 years quantitative research experience.

The researcher/peer reviewer must agree to undertake compulsory training

26.1 The Authority may choose to provide training on the safe handling of the data and disclosure control rules for the outputs of the research to ensure researchers are fully aware of their obligations, and to therefore minimise the risk of disclosure of personal information. Researchers/peer reviewers must agree to undertake any training required by the Authority; failure to do so may constitute grounds for the suspension or removal of accreditation until the training is completed.

The researcher/peer reviewer must agree to their inclusion on a public record

27.1 The Authority is required to publish a register of accredited researchers and peer reviewers. The Authority may also choose to publish a high-level overview of accredited research projects and accredited researchers associated with these projects. Researchers/peer reviewers must consent for these details to be published on the register unless the Authority agrees that there are exceptional reasons not to do so.

The researcher/peer reviewer must sign a declaration

28.1 The researcher/peer reviewer must sign a declaration confirming that they have understood their responsibilities and will abide by the conditions imposed upon them, including protecting the confidentiality of information they access under the Act.

Withdrawal of accreditation

29.1 Accreditation may be suspended or withdrawn from an accredited researcher/peer reviewer for one or more of the following reasons, where the researcher/peer reviewer:

- no longer meets the accreditation requirements;
- fails to have regard to the Code of Practice governing data sharing for research purposes;
- has failed to disclose information that could materially affect the accreditation process or has otherwise dishonestly completed the application form;
- fails to adhere to the terms of any data access agreement between the data holding public authority and the researcher;
- has acted unlawfully in relation to activities for which he or she is accredited;
- has brought the accreditation scheme into disrepute;
- fails to undertake or complete the appropriate training;
- has breached the data protection legislation, or other relevant legislation;
- has been convicted of a relevant offence under the Act, the data protection legislation, or other relevant legislation;
- has had any penalties imposed on it by the Information Commissioner's Office under the data protection legislation; and/or,
- has facilitated or negligently enabled access to identifiable data by a non-accredited person.

Other considerations

30.1 The Authority will provide further guidance on the procedures governing the accreditation of researchers under the Act, including any required training that is a condition of accreditation. In addition to the criteria set out above, applicants should note the following considerations:

- Accreditation as a researcher/peer reviewer will be for a default period of five years. Researchers/peer reviewers are required to renew their accreditation once this term has expired;
- Applicants will be asked to include any relevant information which they think adds or detracts from the application. Steps will be taken during the application process to verify the identity of the applicant;
- Researchers/peer reviewers only need to be accredited once (subject to renewal requirements), but every project requires approval. In line with principle 6 of the Research Code of Practice, accredited researchers/peer reviewers can only use data for the purpose of an accredited research project and that has been processed by an accredited processor(s);
- If the applicant is working towards acquiring the level of skills stated above they may be eligible to apply for provisional accreditation where a fully accredited researcher has agreed to direct, supervise and take responsibility for all work undertaken by the applicant, and on condition the applicant meets the criteria set

out above in a reasonable period of time. This provision does not apply to peer reviewers, who must be fully qualified in their own right; and

- A researcher/peer reviewer who is refused accreditation, or who has their accreditation suspended or removed, will have a right to appeal to the UK Statistics Authority as the accrediting body.
- Details of those researchers/peer reviewers who have had their accreditation suspended or removed may be shared with accredited processors.

Section C: Accreditation of research projects

31.1. Research projects making use of data provided under the Research power must secure accreditation by meeting the following conditions:

Conditions for accreditation of research projects

The research must comply with UK law

32.1 The research must comply with all aspects of UK law, whether enacted by the UK Parliament or, where processing is taking place within the jurisdiction of a devolved administration, by the appropriate devolved legislature. The application must demonstrate to the satisfaction of the UK Statistics Authority that the person(s) that will be involved in the research project will comply with the data protection principles in respect of all forms of personal data, as required by the data protection legislation, , and compliance with them will be monitored.

The research project must be in the public interest

33.1 The Act makes it a condition of the disclosure of data that the research for which the data is disclosed is in the public interest. For the purposes of accrediting research projects the Authority interprets public interest in the same way as 'public good', as set out in the Statistics and Registration Service Act 2007. To secure accreditation, the primary purpose of a research project must therefore be to serve the public interest in one or more of the following ways, to:

- provide an evidence base for public policy decision-making;
- provide an evidence base for public service delivery;
- provide an evidence base for decisions which are likely to significantly benefit the economy, society or quality of life of people in the UK, UK nationals or people born in the UK now living abroad;
- replicate, validate, challenge or review existing research and proposed research publications, including official statistics;
- significantly extend understanding of social or economic trends or events by improving knowledge or challenging widely accepted analyses; and/or

- improve the quality, coverage or presentation of existing research, including official or National Statistics.[11]

The research and its results must be transparent

34.1 The intention and anticipated impact of the research should be set out to the satisfaction of the Authority as part of the application. When the project is complete, all results or outcomes of the research must be made openly and accessibly available in a way that could reasonably be expected to be permanent. The public authority which is the source of the data should be acknowledged to allow others to verify the research. The applicant must also set out a clear commitment to engage with core stakeholders on any useful findings from the research in order to maximise the public benefit.

The research must meet appropriate ethical standards

35.1 The research must meet ethical standards appropriate to the nature and intended use of personal information, for example the Ethical Principles of the National Statistician's Data Ethics Advisory Committee. In assessing whether the research will meet appropriate ethical standards, the Authority may require evidence to be provided to satisfy the Authority that ethical issues have been considered and, where ethical concerns have been raised, that the research proposal includes an appropriate strategy for mitigating or minimising the impact of these concerns. This may include, inter alia, evidence that:

- information that potentially identifies individuals will be stored confidentially and securely;
- issues of consent have been appropriately considered and addressed;
- the risks and limits of new technologies have been considered and appropriately mitigated;
- the research plan provides for human oversight to ensure the methods are consistent with recognised standards of integrity and quality;
- the views of the public have been considered in light of the data used and the perceived benefits of the research; and/or
- the access, use and sharing of data is transparent, and is communicated clearly to the public in an accessible format.

The data requested must be appropriate for the research that is proposed

36.1 The application must demonstrate that the data requested is suitable for the research that is proposed, and that the data requested does not exceed the requirements of the research project.

[11] Whether a given project is accredited or not will be decided on a case by case basis, and will depend on the content and nature of the particular proposal at hand. The above list reflects those attaching to the existing Approved Researcher scheme under the Statistics and Registration Service Act 2007: see https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/approvedresearcherscheme#approved-research-projects

All researchers must be named and accredited

37.1 The project application must name all the researchers who will be accessing the data. No researcher may access the data before they are accredited (including provisional accreditation) under this scheme. When researchers leave or are added to the research project the change must be communicated to the Authority.

Withdrawal of accreditation

38.1 Accreditation may be suspended or withdrawn from an accredited research project accredited for one or more of the following reasons, where:

- the research project is no longer conducted in compliance with the Code of Practice;
- the research project is no longer covered by ethical approval where previously granted;
- the research project is no longer in the public interest;
- a data breach relating to the research project has been reported to the Information Commissioner's Office; and/or
- a court has ordered that the research be halted.

Other considerations

39.1 The Authority will provide further guidance on the procedures and processes governing the accreditation of research projects under the legislation. In addition to the criteria set out above, applicants should note the following additional considerations:

- The application should include an indication of how long the project will take.
- A project can be accredited for a maximum duration of five years, after which the research will require accreditation to be renewed if ongoing access to the data is required.
- The accreditation of research projects can be granted, maintained or withdrawn independently of the accreditation status of researchers or processors involved in the use or processing of data for the project, provided the research project does not breach any of the criteria set out above. This means that withdrawal or refusal of accreditation to a researcher does not necessitate the withdrawal or refusal of accreditation to a research project. Nonetheless, in accordance with Principle 6 of the Research Code of Practice, research can only be conducted where all relevant parties are suitably accredited and only for as long as all relevant parties remain so accredited. Where a research project is refused accreditation, or a project's accreditation is suspended or removed, the applicant(s) will have a right to appeal to the UK Statistics Authority as the accrediting body.