

Data Sharing Code of Practice and Accreditation Criteria: Research

Code of Practice and Accreditation
Criteria for access to data for research
purposes

Date: 19 October 2016

Research: Data Sharing Code of Practice and Accreditation Criteria

© Crown copyright 2016
Produced by the UK Statistics Authority

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/> or email: psi@nationalarchives.gsi.gov.uk <mailto:psi@nationalarchives.gsi.gov.uk>

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

Contents

Part 1 - About the Code of Practice	3
Part 2 – Understanding the power	5
Part 3 – Principles governing the disclosure of data	7
Part 4 - Accreditation criteria	10

Part 1: About the Code of Practice

1. The Act requires three groups of people to have regard to the principles set out in this code of practice:
 - Data holding public authorities in disclosing data for processing, for subsequent research purposes;
 - Processors involved in the processing of 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.
2. The eight principles below are intended to collectively ensure that the processing and provision of de-identified data under the Act is ethical and legal, and done in a way that ensures information that relates to an individual (regardless or not of whether this information identifies the individual) is appropriately protected. All parties involved in the disclosure, processing or use of data under this legislation are required to adhere to these principles in performing their function under the legislation.
3. The Act further requires that all persons or organisations involved in the processing or use of data secure accreditation appropriate to the functions they seek to fulfil under the legislation. Details of the conditions for accreditation are set out under the accreditation criteria.
4. This document has been prepared in accordance with these requirements. 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)
 - Information Commissioner's Anonymisation Code of Practice (2012)
 - Information Commissioner's Conducting Privacy Impact Assessments Code of Practice (2014)
 - Information Commissioner's Privacy Notices Code of Practice (2016)
 - Statistics and Registration Service Act 2007
 - Code of Practice for Official Statistics (2009)
 - Data Protection Act 1998
 - Report of the Administrative Data Taskforce (2012)
 - Cabinet Office Open Data White Paper (2012)
5. The code of practice consists of eight principles, set out below, which apply to all stages in the processing as described in this document, and to the use of de-identified data made available through this gateway. Since there are a number of different ways in which data may be safely and securely processed and used this document does not attempted to provide detailed

guidance on any aspect of the handling or use of data under this legislation. It is instead incumbent on individuals or organisations using this gateway to develop, implement and be able to clearly demonstrate practices and arrangements that fully adhere with the principles described below.

Part 2: Understanding the power

6. Through the Digital Economy Bill [Act 2017] (hereafter the Bill [Act]) the UK Parliament has enacted legislation that facilitates the linking and sharing of datasets held by public authorities for research purposes. The legislation helps to position the UK at the forefront of the international science landscape and supports a number of direct public benefits:
 - increasing the availability of varied and high-quality data for researchers within and outside government will 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 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.
7. The legislation provides certainty and clarity for public authorities and researchers concerning what data can be made available for research purposes and the conditions under which that data can be made available. This will 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.
8. To ensure data are processed and made available in a safe and secure way the legislation sets out six conditions under which this can take place. It also sets out sanctions for those failing to observe the conditions described in the legislation or the principles governing disclosure described below.
9. Section 56 of the Bill [Act] creates a gateway to enable public authorities to make data available to researchers for research that is in the public interest using a trusted third party model. Under this model, a data holding public authority discloses identifiable data to an accredited third party (or the public authority itself acting in this capacity), who is then responsible for processing the data (that is, linking, de-identifying, storing, making data securely available or related procedures) before the de-identified data are made available to a nominated researcher. Section 56(3)-(8) of the Bill [Act] sets out six conditions under which information can be disclosed under this power, specifically that:
 - (1) 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;

Research: Data Sharing Code of Practice and Accreditation Criteria

- (2) The parties involved in processing the data must implement and maintain appropriate safeguards to minimise the possibility that identifying data might be accidentally or intentionally disclosed;
 - (3) The data is made available to the researcher either directly by the person(s) involved in the processing of the data, or, once data are suitably processed, the data holding public authority;
 - (4) 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;
 - (5) The researcher(s) and all persons involved in processing the data are accredited for these functions; and
 - (6) 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.
10. Section 61 identifies the UK Statistics Authority (hereafter the Authority) as the body responsible for overseeing the accreditation processes set out in the Act.
11. Section 60(1) of the Bill [Act] establishes the requirement that the Authority prepares and publishes a code of practice concerning the disclosure, processing, holding and use of information under this gateway. The Authority must consult publicly before issuing or reissuing this code, and must lay the code before the UK Parliament and the legislatures of the devolved administrations in Scotland, Wales and Northern Ireland.
12. The Bill [Act] further obliges 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 legislation.

Part 3: Principles governing the disclosure of data

Principle 1: Legal

13. Data can only be disclosed to processors (for the purpose of subsequently making de-identified data available to researchers) where expressly permitted through the meeting of the six conditions set out at section 56 of the Digital Economy Bill [Act 2017], or through appropriate secondary regulations, as established by the Westminster Parliament or the legislatures of the Devolved Administrations in Scotland, Wales and Northern Ireland. Data holders, processors and researchers must also ensure they adhere to the legal requirements set out in the Data Protection Act 1998 and Part 1 of the Regulation of Investigatory Powers Act 2000, and are expected to have regard to best practice on privacy impact assessments and privacy notices, as established in the ICO's Conducting Privacy Impact Assessments Code of Practice and Privacy Notices Code of Practice.

Principle 2: Accreditation

14. All accredited persons and the research project 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 available data to other processors or researchers it is done for the specific purposes set out in the Bill [Act] and only to a person that is accredited for the function they are fulfilling. The UK Statistics 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 accreditation applicants (or those whose accreditation is suspended or removed) have recourse to appropriate appeals mechanisms.

Principle 3: Data security and confidentiality

15. All parties and persons disclosing, making data available, processing or using data under the provisions set out in the Bill [Act] must ensure they do so in a way that never compromises the confidentiality of personal information. Appropriate safeguards must therefore be established and maintained at all stages and by all parties and persons involved in the disclosure or processing of data and their use for research purposes. Before providing accredited researchers access to data, processors must ensure the data has undergone a process of disclosure control that is commensurate and proportionate with the sensitivity of that data. All persons handling data must ensure the integrity of these safeguards is maintained by proactively identifying privacy and security risks and regularly

reviewing safeguards and security solutions to ensure they continue to meet the challenges posed by evolving technologies.

Principle 4: Public interest

16. Data obtained under this legislation must only be disclosed, processed and used for the purpose of supporting research in the public interest. Research in the public interest is research that will, for example:

- provide or improve evidence bases that support the formulation, development or evaluation of public policy or public service delivery;
- guide critical decision-making with anticipated impacts on the UK economy, society or quality of life of people in the UK;
- significantly extend existing understandings or social or economic trends or events, either by improving knowledge or challenging accepted analyses; or
- replicate, validate or critically analyse existing research (including official statistics) in a way that leads to improvements in the quality, coverage or presentation of existing research.

17. The UK Statistics Authority has set out further information concerning the criteria for determining whether research is in the public interest under the criteria for the accreditation of research projects, set out below.

Principle 5: Ethical

18. All parties must ensure that they observe the highest ethical standards when sharing, processing or making use of data under this gateway. They must ensure that the unique ethical challenges presented by using data collected for operational reasons and held by public authorities are reflected and accounted for in the discharging of each of the functions described within the Bill [Act]. This will involve, principally, 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 or made available. 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 6: Proportionality and minimised burdens

19. 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, whether those burdens and costs are accrued by the public authority acting as a data holder, the public authority or trusted third party acting as a processor, or the researcher(s). A researcher should ensure that in seeking to secure access to data held by public authorities he or she has assessed, in so far as he or she is able, suitable, less burdensome alternatives and is satisfied that no alternatives exist or that the financial or quality costs of securing data from other sources would be prohibitive.

Equally, data suppliers 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 7: Retention and onward disclosure

20. Third party data processors can only retain pre-processed, identified data for a limited time. The UK Statistics Authority will set out this period as part of the accreditation process 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).
21. Processors who store the de-identified data may make that de-identified data available to other researchers and for other research projects within this time period only where the following criteria are met:
 - the data supplier has agreed to the processor making 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.
22. In line with the requirements set out under Principle 2, under no circumstances should data be disclosed, made available in de-identified form or passed to any parties who are not suitably accredited.

Principle 8: Transparency

23. All parties should adopt a commitment to transparency, where possible, to maximise the potential public value of research facilitated by access to public data. Researchers should engage core stakeholders on the findings of the research drawn from these data, and ensure that research findings are made freely available to the public. Data supplying public authorities and processors may also choose to publish information about the data they are making available, the rationale and purpose of doing so, and any restrictions and safeguards associated with the processing and use of those data. Considerations of whether or not to publish such information should be balanced with security or other considerations where the risks of publishing such information would outweigh the potential public benefits. In its accreditation capacity, the UK Statistics Authority may also chose to publish details on accreditation applications and outcomes, including the outcome of any appeals process, in accordance with its statutory responsibilities.

Part 4: Accreditation Criteria

Accreditation of processors

24. The disclosing and provision of data held by public authorities for the purpose of conducting research in the public interest, as set out in the legislation, is conditional on the data being processed by an accredited processor. A processor must be accredited for one, or both, of two functions, specifically:
- (i) the linking, matching and de-identifying of data (hereafter referred to as the preparation of de-identified data); and/or
 - (ii) the storing and provision of access to data (hereafter referred to as the provision of de-identified data).
25. Any person(s) involved in either the preparation or provision of data under this legislation must be accredited for the appropriate function (or both), as appropriate. Accreditation documents will clearly state for which of these functions the processor has been accredited. The UK Statistics Authority will also publish details of accredited processors, along with details of which function(s) the accreditation covers.
26. In some cases, the processor could be the public authority whose data has been requested if they have the necessary expertise. To maintain standards and consistency throughout the accreditation process public authorities processing 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.
27. By default, an accredited processor will retain accredited status for five years, or 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 a processor. In such circumstances the UK Statistics Authority may decide to provide notice of its intention to suspend and reassess the accreditation status of processors.
28. To secure accreditation processors must meet the following conditions:

The processor must be based within the territorial jurisdiction of the UK

29. To ensure processors are legally accountable for the work they carry out under the legislation only processors based in the UK are eligible for accreditation. The processor must in addition provide a guarantee, at the

point of accreditation, that it will carry out all of its processing within the UK. The processor must be able to provide evidence on request that this is the case in order to maintain its accredited status.

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

The processor must have appropriate skills and experience

30. 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 the data should also have security clearance appropriate to the nature of the data they are handling.
31. The processor must agree to maintain a list of all those individuals who meet these requirements, and to ensure that individuals are only involved in aspects of the processing for which they are suitably experienced and trained and that only these individuals have access to data provided by the public authority. A processor must also agree to ensure that all individuals involved in any aspect of the processing have signed a declaration to say that they understand their responsibilities.

The processor must make use of appropriate technical infrastructure

32. The processor must make use of 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

33. 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 this legislation. 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.

34. The processor must ensure that adequate data processing agreements are in place for any data they receive from public authorities before they process that data. The processor must also agree to abide by any additional policies and procedures the UK Statistics Authority in its accreditation capacity may develop and set out from time to time. The Authority will provide appropriate notice where it intends to introduce new policy requirements.

The processor must comply with UK law

35. The processor must undertake to comply with all aspects of UK law set out in primary and secondary legislation, whether enacted by the Westminster 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 Data Protection Act (1998), the Human Rights Act (1998), the Statistics and Registration Service Act (2007), and Part 1 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 agree to its inclusion on a public register

36. The UK Statistics Authority is required to maintain a public register of accredited persons. Any persons seeking accreditation for processing under this legislation must therefore agree to their inclusion on this register.

The processor must consent to being audited

37. In order to discharge its duty of oversight and ensure processors continue to meet these requirements the UK Statistics Authority may, from time to time, decide to undertake an audit of accredited processors. Processors are required to consent to be audited during its accreditation application, and must fully comply with any audit that takes place in order to maintain its accredited status.

The processor must commit to having regard to the Code of Practice

38. The processor must undertake to adhere to the principles set out in the code of practice when fulfilling any of its processing functions. Compliance may be assessed by an audit and is a central condition for the maintenance of a processor's accredited status.

Withdrawal of accreditation

39. Accreditation may be suspended or withdrawn from a processor accredited for the preparation or provision of data for any or multiple of the following reasons:

- Failure to have regard to the code of practice under section 60 of the Digital Economy Bill [Act 2017];
- Conviction for offences under the Data Protection Act;
- Penalties imposed by the Information Commissioner's Office relating to processing under section 56 of the Digital Economy Bill [Act 2017];
- A reported or suspected data breach
- Failure to meet accreditation requirements;
- Refusal to provide, or withdrawal of, the processing service for which it has been accredited;
- Refusal to be audited, or obstruction of the auditing process; and/or
- Charging fees for processing, other than those ordinarily permitted for cost-recovery purposes.

Other considerations

40. The UK Statistics 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 legislation.

Accreditation of researchers

41. Researchers undertaking research using data provided under the gateway set out in part 5, chapter 5 of the Digital Economy Bill must secure accreditation by meeting the following conditions:

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

42. To ensure a researcher has the necessary skills to make suitable use of the data they must be able to demonstrate through example(s) the following skills;

- Evidence gathering
- Literary review
- Interpretation & analysis of data
- Drawing conclusions
- Presentation of results

The researcher must agree to undertake compulsory training

43. The UK Statistics Authority (or its partners) may choose to provide training on the safe handling of the data and disclosure control rules for the outputs to ensure researchers are fully aware of their obligations, and to therefore minimise the risk of disclosure of personal information. Researchers must agree to undertake any training required by the Authority. Failure to undertake this training may constitute grounds for the suspension or removal or accreditation until the training is completed.

The researcher must agree to their inclusion of a public record

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

The researcher must sign a declaration

45. The researcher 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 legislation.

Withdrawal of accreditation

46. Accreditation may be suspended or withdrawn from an accredited researcher for any or multiple of the following reasons:
- Failure to have regard to the code of practice under section 60 of the Digital Economy Bill [Act 2017];
 - Failure to disclose information that could materially affect the accreditation process (such as a previous conviction under the Digital Economy Bill [Act] s.58(5) or 59(4); or under the Data Protection Act), or dishonestly completing the application form;
 - Failure to adhere to the terms of any written data access agreement between the data holding public authority and the researcher;
 - Acting unlawfully in relation to activities for which he or her is accredited;
 - Bringing the accreditation scheme into disrepute;
 - Failure to undertake or complete the appropriate training; and/or
 - Deliberately facilitating or, through negligence, enabling access to the data by a non-accredited person.

Other considerations

47. The UK Statistics Authority will provide further guidance on the procedures governing the accreditation of researchers under the legislation, including any 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 will be for default period of five years. Researchers 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 only need to be accredited once (subject to renewal requirements), but every project requires approval. In line with principle 2 of the code of practice accredited researchers can only use data for the purpose of an accredited research project and that has been processed by an accredited processor;
- 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 criteria 2 to 4 set out above; and
- A researcher who is refused accreditation, or who has their accreditation suspended or removed will have a right to appeal.

Accreditation of research projects

48. Research projects making use of data provided under the gateway set out in part 5, chapter 5 of the Digital Economy Bill must secure accreditation by meeting the following conditions:

The research must comply with UK law

49. The research must comply with all aspects of UK law set out in primary and secondary legislation, whether enacted by the Westminster 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 proposed research project will meet the data protection principles as set out in the Data Protection Act and monitored by the Information Commissioner's Office.

The research project must be in the public interest

50. The legislation 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 UK Statistics 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 projects 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;
- to provide an evidence base for public service delivery;
- to 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;
- to replicate, validate or challenge existing research, including official or National Statistics;
- to significantly extend understanding of social or economic trends or events by improving knowledge or challenging widely accepted analyses; and/or
- to improve the quality, coverage or presentation of existing research, including official or National Statistics.

The research and its results must be transparent

51. The intention and anticipated impact of the research should be set out to the satisfaction of the UK Statistics Authority as part of the application.

52. When the project is complete, all results or outcomes of the research must be made freely 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 have ethical clearance from a recognised body

53. The research must be reviewed and approved by a body that is suitably qualified and appropriate to review the ethical considerations of the proposed research (such as a university ethics committee or an independent body). In addition to demonstrating how the proposed research serves the public interest and is fully compliant with UK law (see above), applications will need to demonstrate that:

- Potentially disclosive information 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;

Research: Data Sharing Code of Practice and Accreditation Criteria

- 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;
- The access, use and sharing of data is transparent, and is communicated clearly and accessibly to the public.

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

54. 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.

All researchers must be named and accredited

55. The project application must name all the researchers who will be accessing the data. No researcher may access the data before they are accredited under this scheme. When researchers leave or are added to the research project the change must be communicated to the UK Statistics Board.

Withdrawal of accreditation

56. Accreditation may be suspended or withdrawn from an accredited research project accredited for any or multiple of the following reasons:

- Failure to have regard to the code of practice;
- The research project is no longer covered by ethical approval;
- Information comes to light, or the research project changes, so that the project can no longer be considered to be in the public interest;
- A reported or suspected data breach;
- A court ordered that the research be halted.

Other considerations

57. The UK Statistics 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 data will be needed for. To comply with the Data Protection Act, and in accordance with principle 7 of the Code of Practice, data will be destroyed once it is no longer needed for the accredited research project, unless an extension of retention has been granted.

Research: Data Sharing Code of Practice and Accreditation Criteria

- A project can be accredited for a maximum duration of five years, after which the research will require reaccreditation if ongoing access to the data is required.
- A research project can remain accredited even where accreditation is withdrawn from the organisation processing data for the project, or from the researchers carrying out the project, provided the research project does not breach any of the criteria set out above.