Office for National Statistics

ons.gov.uk

[ONS Research and Data Access Policy]

Contents

Policy name	ONS Research and Data Access Policy
This policy has been authorised by (SRO)	Pete Stokes
Policy owner	Research Support and Data Access
Scope of the policy	Office for National Statistics
Release Version	Version 1.0
Status	Approved

1. Introduction

ONS is committed to providing access to unit-record de-identified survey and administrative data for statistical research that delivers a public benefit for the UK and where access is granted to researchers in a safe and consistent way, in line with legislation and ONS policies. We believe that better statistics lead to better decisions and that the research community is pivotal to achieving our national goals. Their research helps the UK understand and make informed decisions regarding the economy, society and people's quality of life.

This policy provides certainty and clarity on the governance arrangements adopted by ONS for access to data for research purposes, including the conditions under which access to these data is granted and the framework for accrediting researchers, research projects and data processors. This will help to ensure a consistent and transparent approach for access to data for research purposes so that the benefits are more easily realised and the confidentiality of the data is protected. The policy takes account of Part 5 of the Digital Economy Act 2017 that facilitates the linking and sharing of datasets held by public authorities for research purposes.

2. Background

In making unpublished data available for research, ONS gives detailed consideration to the analytical needs of researchers and the controls governing their use are set according to the risk to data confidentiality. We must strike the correct balance between maximising the utility of the data and protecting the confidentiality of data subjects (individual and body corporate). For example, the more detailed the data, the greater the risk of a person being identified and more significant controls on data access and research outputs are applied accordingly. This spectrum of data access is shown in figure 1 on page 11. The risk of identification in the most detailed 'controlled' data means these data are considered 'personal information'

as defined in the Statistics and Registration Services Act 2007 (SRSA), and require legal protection.

Access to Personal Information which is held by the UK Statistics Authority for the purpose of enabling or assisting its functions, may be granted by ONS on the Authority's behalf, under the SRSA. Personal information is defined as information that relates to, and identifies a particular person (including a body corporate), if the identity of that person:

- is specified in the information,
- can be deduced from the information, or
- can be deduced from the information taken together with any other published information.

It does not include information about the internal administrative arrangements of the Authority.

To ensure there are rigorous arrangements to protect data confidentiality in accordance with the SRSA and the UK Statistics Authority's Code of Practice for Official Statistics, ONS has adopted a "five-safes" model. The model articulates our arrangements to ensure safe people, safe projects, safe settings, safe outputs and safe data. It is described in more detail in the principles section (paragraphs 6.1 – 6.18).

In addition to the powers available under the SRSA, ONS may also grant access to personal information to researchers (individuals and/or organisations) through other UK legislation, including the Statistics of Trade Act (STA), 1947 and the Digital Economy Act 2017 (DEA). Further information on these legal gateways is described in the practices section (paragraphs 5.2 – 5.8).

In accordance with the DEA Research Code of Practice and Accreditation Criteria, ONS has adopted principles governing our management of research data access and the protection of data confidentiality. These are set out in the principles section (paragraphs 6.19 – 6.35).

The policy should be considered in relation to other relevant ONS data policies, including, but not limited to, the following:

- A secure environments policy setting out details of the physical environment and processes in place to meet the requirements to hold sensitive data;
- A major incident protocol related to data security and privacy breaches
- A de-identifying data policy; and

- A data retention and destruction policy.

Action taken in relation to suspected non-compliance with this policy is set out in the Research Data Access and Accreditation: Non-Compliance and Breaches Policy (Annex A).

3. Scope

This policy applies to the access to unpublished data (survey and/or administrative data, either used on their own or linked) for statistical research and the accreditation of researchers, projects and processors in relation to this access. It applies to:

- Access to ONS survey and administrative data managed by ONS or other organisations (data processors) on behalf of ONS;
- Access to research data managed by ONS on behalf of other data owners in the Secure Research Service;
- Access to data owned by Public Authorities and made available to researchers through the DEA and managed by ONS (but not necessarily hosted by ONS in the Secure Research Service); and
- The accreditation of researchers, projects and processors for the access listed in 3.1, through the SRSA, DEA and other relevant legislation.

4. Objectives

The purpose of this policy is to ensure that:

- ONS has effective, accountable and transparent arrangements in place to manage access to data held by ONS and/or other public authorities, for statistical research that delivers a public benefit to help ensure data confidentiality is protected;
- ONS has effective arrangements in place for the accreditation of researchers, research projects and data processors in accordance with the SRSA 2007 and DEA 2017;
- ONS takes transparent, consistent, proportionate and targeted action to deal with suspected breaches of lawful research data access and/or non-compliance with the conditions of data access, to help ensure data confidentiality is protected;
- The roles and responsibilities of all parties in the research and analysis community involved in access to ONS data for research, are clearly defined and set out, and are understood (i.e. researchers understand the action that ONS takes and why in response to data breaches);

- ONS, working with the research and analysis community, demonstrates the impact of research carried out using unpublished data to help provide assurance to data subjects, data owners and others that their data is being used safely and in a way that delivers a public benefit; and
- ONS arrangements for managing research data access are consistent with those adopted by other administrative research centres and data controllers.

5. Practices

The Research Data Access Community

There are a range of persons/organisations with an interest in the use of unpublished data for statistical research. These stakeholders have specific duties, interests and involvement, as follows:

- **Data owners** make their data available for statistical research that delivers a public benefit. They may manage access to their data using their own systems (e.g. in a safe setting such as the Secure Research Service or available as download for safeguarded data), or make their data available to a data processor on their behalf (e.g. ONS deposits secure and safeguarded data with the UK Data Service). Data owners may set out specific conditions for access to their data, for example, defining the safe settings for where the data may be accessed or setting out how research projects and researchers will be accredited. For access to data to be granted, the Information Asset Owner (IAO) from the relevant data owner, must agree to its use for the purpose specified. The IAO may delegate this responsibility to a data processor if they wish.
- **Data controllers** are persons who (either alone, or jointly, or in common with other persons) determine the purposes for which, and the manner in which, any personal information are processed. They may have delegated authority to perform this role on behalf of a data owner. If two datasets are linked or matched, then both data owners will be data controllers.
- **Accredited Data Processors** may perform the functions of: the preparation of de-identified data for the purposes of data linking, matching, de-identifying, storing or related procedures before the de-identified data are made available for research purposes in a secure environment. The data processor can either be an accredited third-party or the data-holding (data owner) public authority itself. Processors will carry out data disclosure control practices to minimize the risk of the data being

identified following publication of research results. Data processors may carry out clearance checks (see safe outputs) if they have been approved to perform this function.

- **Accredited Researchers** may access data as an individual or on behalf of an organisation. Traditionally, most access to ONS data by researchers from non-government organisations, is granted to individual accredited researchers through the Approved Researcher scheme. However, there may be times when these researchers can access data on behalf of government (e.g. under contract), under the conditions that apply to these organisations. Government researchers may access data individually (e.g. through a legal gateway such as the Approved Researcher scheme) or at an organisation level (e.g. through the terms of a Ministerial Direction with the UK Statistics Authority). The type of access is usually dependent on the specific data they wish to access and the specific conditions for access set out by the IAO. Further details on the criteria for researcher accreditation are set out in paragraphs 6.2 – 6.5 (safe people).
- **Research sponsors** are organisations that commission research. They may be government departments that have contracted a specialist research company to evaluate their policies or an organisation that doesn't have the specific skills to carry out the research themselves. Decisions on how and where the research findings are published and ownership of the analysis, may be determined by the sponsors.
- **Data approvers** include data owners, administrators and committees that consider and accredit researchers, research projects or data processors. The ONS approval committees include the Microdata Release Panel (MRP) for access to ONS research data and the National Statistician's Data Ethics Advisory Committee (NSDEC) which gives ethical, public benefit and transparency advice on research projects. The MRP will be superseded at the end of 2018 by the independently chaired Research Accreditation Panel (RAP) which will consider all requests for ONS and Public Authority data for research, via the legal gateways set out in paragraphs 5.2 – 5.8.
- **Data consumers** are unlikely to be involved in carrying out or commissioning research, but may have an interest in the findings. They might include journalists, policy or community organisations with an interest in a specific topic. They use the outcomes from research to inform democratic debate and raise awareness and understanding about specific issues.

Legal gateways for data access - Legislation

Data classified as personal information under the SRSA and other relevant legislation, has legal protection. For access to these data to be granted, there must be a legal gateway.

ONS grants access to data for research using a number of different legal gateways, as follows:

The Statistics and Registration Service Act, 2007

The SRSA established the UK Statistics Authority. It contains specific provisions governing the use, the confidentiality of personal information held by the UK Statistics Authority and ONS and penalties for any unauthorized disclosure. Section 39 sets out the provisions for access to unpublished data by fit and proper persons (Approved Researchers, section 4(i)) and to approved organisations (government organisations, (subsection 4(h)) with the consent of the person to whom it relates, for the purpose of statistical research. Subsection 4(c) allows ONS researchers, or researchers working on behalf of ONS, to access the data for the purpose of enabling or assisting the UK Statistics Authority to exercise any of its functions;

ONS grants access to our social survey data to **Approved Organisations**, as permitted by s.39 SRSA the Statistics and Registration Service Act 2007 (SRSA) (section 39). ONS defines approved organisations as UK government departments, agencies and other public bodies, including the devolved administrations in Northern Ireland, Scotland and Wales, which produce official statistics and/or undertake statistical analysis required for government policy development and/or decision making. All applications for access to these data are considered by the ONS Microdata Release Panel (MRP) and, if approved, a Data Access Agreement is put in place to set out the conditions of access. A list of all approved organisations accessing ONS research data via this gateway is published on the ONS website.

Subsection 42 (4) of the SRSA sets out that organisations specified in the Act or subsequent legislation, may access ONS births and death registration data to support the functions and performance of the health service. Organisations specified by the Secretary of State for Health and Social Care can apply to access these data through this gateway.

Statistics of Trade Act, 1947

Disclosure of data via **Ministerial Direction** (MD) is permitted under provisions within the Statistics of Trade Act 1947 (STA), which legislates for the obtaining of information **by government departments** to help government understand economic trends and provide a statistical service for industry. Government departments may apply to access ONS business survey and/or administrative data via a Ministerial Direction and these applications are considered by MRP and its successor the DEA Research Accreditation Panel (RAP). The MD is signed on behalf of the UK Statistics Authority by the National

Statistician, and details of access to ONS data through this gateway are published on the ONS website

The Employment and Training Act, 1973 (ETA)

The ETA, as amended by the Employment Act 1988) grants local planning bodies the authority to develop **Local Development Plans**. Specific provisions within this legislation enable local authorities access to some parts of the Inter-departmental Business Register (IDBR). This is produced using data collected from businesses surveys under the Statistics of Trade Act 1947 (STA).

Digital Economy Act, 2017

Provisions within the Research Code of Practice and Accreditation Criteria of the **Digital Economy Act, 2017** facilitates the linking and sharing of data held by public authorities for research purposes that delivers a public benefit. The Act requires the UK Statistics Authority to issue a Code of Practice setting out the arrangements for the disclosure, processing, holding or use of personal information under this gateway. The Act requires three groups of people to have regard to the principles set out in the Code: data-holding public authorities disclosing personal information; accredited data processors; and accredited researchers accessing the data for the purpose of research. This research data access and accreditation policy is consistent with the DEA Research Code of Practice and Accreditation Criteria.

6. Principles

Safe Use of ONS data

To ensure rigorous arrangements are in place to protect data confidentiality, ONS has adopted a “five-safes” model. The model is predicated on the basis that safe use of the data will be achieved by having:

- Safe people – only accredited researchers can access the personal information
- Safe project – only accredited research that is feasible, lawful and provides a public benefit will be permitted
- Safe setting – in a secure environment such as the ONS Secure Research Service
- Safe data – the access arrangements for the data will be commensurate with the risk of data disclosure

- Safe outputs – thorough checks of research outputs and code are in place to protect data confidentiality

Application of the ONS Five Safes model ensures data are processed and made available to accredited researchers in a safe and secure way that is consistent with the conditions for the disclosure of personal information set out in the DEA. These are as follows:

- 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 the DEA Research Code of Practice and Accreditation Criteria.

Safe People

The SRSA sets out that ONS will grant access to individuals considered a 'fit and proper person' and that it will publish criteria setting out what constitutes a fit and proper person, e.g. an Accredited Researcher. These researchers must have an interest in accessing the data to serve the 'public good'. They must demonstrate safe attitudes and behaviours to ensure they handle data securely and protect the confidentiality of data subjects.

The ONS and DEA criteria to be an accredited researcher is:

- Evidence of suitable research qualifications or a minimum of three-years quantitative research experience;
- Successful completion of the Safe Researcher training to ensure they have the right attitude towards data access and right behaviours to use data safely;
- Agreement to their inclusion on a public record of accredited researchers, unless there are exceptional reasons not to do so; and

- Signed declaration confirming they have understood their responsibilities and will abide by the conditions imposed upon them, including protecting the confidentiality of data subjects.

Accreditation as a researcher will be for a default period of five years. Researchers will be required to renew their accreditation once this term has expired, if they wish to continue to access personal information. If a person is working towards acquiring the level of skills to be eligible as a full accredited researcher or perform the functions of preparing and handling the data (rather than carrying out quantitative analysis), they may be eligible for provisional accreditation where a fully accredited researcher has agreed to direct, supervise and take responsibility for all work undertaken by the applicant. Provisional accredited researchers will be required to meet all the same conditions as fully accredited researchers except the research qualification/experience requirement.

Accreditation may be suspended or withdrawn if the researcher fails to comply with the terms and conditions of their access. More information is set out in the Research Data Access: Non-compliance and breaches policy.

Safe Projects

For access to data to be granted and used for the purpose of supporting research in the public interest, researchers must demonstrate that their research:

- is a feasible, lawful and ethical use of the data;
- requires access to the level of detail they are requesting;
- will deliver clear public benefits to the UK; and
- is transparent use of the data, i.e. they will publish their results to enable use, scrutiny and further research.

To be a feasible use of the data, there should be a clear and defined scope, realistic and time bound period of access, and appropriate use.

To demonstrate a public benefit, the purpose of research must demonstrate at least one of the following criteria:

- provide or improve evidence bases that support the formulation, development or evaluation of public policy or public service delivery;
- To provide an evidence base for decisions which are likely to significantly benefit the UK economy, society or quality of life of people in the UK;
- significantly extend existing understanding of social or economic trends or events, either by improving knowledge or challenging accepted analyses; or,

- replicate, validate, challenge or review existing research (including official statistics) in a way that leads to improvements in the quality, coverage or presentation of existing research.

There must also be a legal gateway through which access may be granted. The legislation sets out the conditions under which access may be granted and may apply to individuals or organisations. More information about the legal gateways for data access are set out in paragraphs 5.1 – 5.8.

Governance arrangements for managing access to data for research are determined by the data owner. Applications for access to research data owned or managed by ONS are reviewed by the Microdata Release Panel (MRP). Membership is drawn from ONS data owners together with other subject matter experts, such as Information Assurance, Methodology, etc. MRP will be superseded by a Digital Economy Act Research Accreditation Panel (RAP). All DEA applications will also be considered by the National Statistician's Data Ethics Advisory Committee for ethical advise.

Safe Setting

Once a project is approved, we still need to ensure that data are safe, so we don't give the researchers a copy if its personal information. As there is an inherent risk of identification of data subjects, we only make personal information (with direct identifiers removed) available to researchers outside of government in a secure research setting, such as the ONS Secure Research Service (SRS) or the UK Data Service Secure Lab. Researchers can analyse data on these systems, but do not have access to email, the internet, printers or any other way of taking out the protected data. The SRS system has a wide range of security controls built in, including CCTV in the secure rooms and protective monitoring software, which monitors and records every keystroke and mouse-click researchers make to ensure nobody misuses the data.

ONS permits access to the SRS either at a safe setting location or via a remote connection to trusted organisations and for trusted devices. ONS will publish criteria setting out what constitutes a trusted organisation and device, and these will reviewed from time to time to ensure they remain up to date.

Safe Data

Data published on the ONS website are subject to strict statistical disclosure control methodologies to ensure full confidentiality, and their use is virtually unrestricted as specified by the terms of the Open Government Licence. De-identified research data, with significant restrictions on key variables (e.g. age and geography) and therefore with very little risk of identification, are available for statistical research purposes only, under the terms of an **End**

User Licence (EUL). Researchers must sign up to those terms before being permitted to download a copy of these 'safeguarded' data from the UK Data Service. Researchers accessing these safeguarded data do not need to be accredited.

De-identified microdata with little or no restrictions on the variables or geographic information provided are also made available for statistical research, but their use is heavily **controlled**. There is a significant risk that data subjects could be identified, making these data Personal Information and protected under the SRSA. The principle legal gateway required to grant access is the ONS **Approved Researcher** scheme. These data should be analysed within a secure environment, such as the SRS or UK Data Service Secure Lab. ONS previously permitted the use of less detailed data by Approved Researchers, with fewer restrictions, as downloads under the terms of a Special Licence from the UK Data Service and analysed on researchers own systems. A review of the level of detail provided in these Special Licence data concluded that they were "Personal Information" and therefore required a legal gateway for access. A recent review (including a public consultation) of the Approved Researcher scheme concluded that Accredited Researchers should only access personal information in a secure environment. ONS has therefore stopped further access to Special Licence data as a download and these data, together with more detailed research data, are now available in the SRS and Secure Lab.

Safe Outputs

As researchers cannot take research data out of the safe setting such as the SRS, the outputs from their analysis need to be checked using statistical disclosure control methods to ensure that data subjects are not identified in the data or that attributes about them are not discovered from the research findings. This ensures that outputs are non-disclosive and data confidentiality is protected. There are three types of clearance.

Researchers can request pre-publication clearance when they wish to remove files from the SRS for writing up results, or for further discussion with members of the project team, including project sponsors. Cleared pre-publication outputs must not be published.

A publication clearance is the final intended output from research, that a researcher wishes to publish or share beyond the research team. This can be in the form of a report, publication, presentation, speech, etc, and must include everything that will be disseminated including graphics and text. The third type of clearance is for code files. These code files may be shared freely once approved, and must not contain identifiers or any commands that may attempt to search or identify individual entities.

Output and/or code file clearances must only be carried out by accredited processors or output checking experts, once they have completed the ONS output checking course.

Principles governing the disclosure of data

We will apply the principles of data access for research purposes set out in the DEA Research Code of Practice and Accreditation Criteria, to ensure that the processing and provision of personal information is ethical and legal, and done in a way that ensures information that relates to an individual or body corporate, is adequate protected. ONS will adhere to the principles in order to meet our duties for disclosing, processing or using data for statistical research. We will also adopt these principles in relation to the disclosure of non-personal information (e.g. safeguarded data under the terms of an End User Licence) as a matter of good practice.

Principle 1: Confidentiality

We will ensure, as far as is practicable, that all persons disclosing, making data available, processing or using data under the provisions set out in relevant legislation (e.g. Statistics and Registration Services Act, 2007; Digital Economy Act, 2017) do so in a way that protects the confidentiality of personal information and personal data. We will ensure that all persons involved in access to these data, maintain the data safeguards by proactively 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. Protecting data confidentiality is an integral component of the Safe Researcher training that all accredited researchers need to successfully complete and is a condition of their access to the data. Maintaining the integrity of data safeguards and protecting data confidentiality is integral to the accreditation of data processors.

Principle 2: Transparency

To maximise the public benefit of research facilitated by access to research data and build trust in its use, we are committed to ensuring there is transparent use. It will be a condition of access to these data, that researchers make the findings from their analysis openly and publicly available, wherever possible. We may grant exemptions to publishing this information in exceptional circumstances, which could include security concerns around naming individuals, or a need for confidentiality of sensitive policy development within government. All exemptions will be submitted to the ONS Microdata Release Panel or similar approval committee for their view. We will work with other public authorities and the wider research data access community to promote transparency in the use of the data and publication of research findings in the public domain.

We will maintain public records of all data we make available for research, including details of the organisation/researcher, a synopsis of the data they are accessing and the purpose of their analysis.

Principle 3: Ethical use and the law

Data will only be disclosed to processors (for the purpose of subsequently making de-identified data available to researchers) where expressly permitted by both the data owner and accrediting organisation, and processors must comply with the conditions set out for a processor. In disclosing data, we will work with data holders, processors and researchers to ensure they meet all legal obligations arising from the Data Protection Act and other applicable legislation.

We will ensure that all parties involved in the disclosure, processing or use of data through the relevant legislation, including ONS, observe the highest ethical standards, ensuring that the unique ethical challenges presented by using data collected for operational purposes are accounted for and addressed. Working with RAP and NSDEC, we will ensure 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. We will ensure that a mechanism is in place whereby all accredited research projects are approved for the ethical use of the data requested, either by RAP or NSDEC, or an ethics committee connected with an institution carrying out/supporting the research.

Principle 4: Public interest/good

ONS 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. This is described in paragraph 6.9 of this policy.

Principle 5: Proportionality

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. We anticipate that a researcher should ensure that in seeking to secure access to data held by public authorities, they have assessed, insofar as they are 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.

ONS also applies the principle of proportionality in taking action in response to suspected breaches of data confidentiality. Further information is set out in the Research Data Access and Accreditation: Non-compliance and Breaches Policy.

Principle 6: Accreditation

All accredited persons working on a 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 required to ensure that where they disclose or make data available to other processors or researchers, it is done for the specific purposes set out and only to a person that is accredited for the function they are fulfilling.

ONS 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 applicants (or those whose accreditation is suspended or removed) have recourse to appropriate appeal mechanisms.

ONS will publish criteria and guidance on the accreditation of persons, projects and processors. These will set out the accreditation processes so that users know what to expect and can hold ONS to account if its performance falls short of expectation. To ensure that ONS processes and access to research data is transparent, ONS will publish and update:

- Criteria for accreditation and withdrawal of accreditation
- A list of persons and organisations with access to ONS research data and the purpose for which access has been granted
- Details of the service we will provide to accredit persons, persons and processors
- Details of the conditions that we associate with accreditation, e.g. full researcher accreditation will last for a period of five years;
- This Research Support and Data Access Policy and the annexed Non-compliance and Breaches Policy; and
- Details of the process for appeals against decisions on the accreditation of researchers, projects and/or processors.

Principle 7: Retention and Onward Disclosure

Third party data processors can only retain pre-processed, identified data for a limited time as necessary for them to discharge their function. ONS will take account of guidance issued by the UK Statistics Authority on the accreditation of processors under the Digital Economy Act.

As a data processor under the SRSA, ONS makes de-identified data available to researchers and for research where the following criteria are met:

- the data supplier has agreed to let ONS make the de-identified data available to additional individuals and/or for additional research projects;
- ONS remains fully accredited as a data processor for its disclosure function; and,
- the researcher and the research project are fully accredited for the use of these data.

Data processors must ensure 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.

Relationship with other data policies

This policy should be considered with reference to other ONS data policies, including:

- Data Retention and Destruction
- ONS Secure Environments Policy
- ONS Data Linking and Matching Policy
- ONS Data De-identification Policy

Non-compliance with this policy

Despite the rigorous arrangements in place to protect confidentiality, there is still the possibility for a breach to occur when an individual or organisation does not fulfill their responsibilities – willfully or unintentionally. The ONS Research Data Access and Accreditation: Non-compliance and Breaches Policy sets out our approach for dealing with non-compliance with the legal requirements and/or conditions of access under which access to the data was granted, including any of those circumstances set out in the DEA Research Code of Practice and Accreditation Criteria. The policy includes non-compliance with the procedures and agreements in place for data access, which might result, in the worse-case scenario, in the loss or disclosure of data. The policy includes details of: the types of

breaches; the principles we will apply when investigating suspected breaches; and the appeals process.

8. Appeal Process

A researcher or organisation has a right to appeal if they disagree with a decision by ONS to approve, withhold or withdraw researcher accreditation, or take action against a researcher/organisation following investigation of suspected non-compliance. Examples of when a researcher might submit an appeal include:

- The researcher/organisation disagrees with the decision not to approve accreditation of a researcher and/or project;
- The organisation disagrees with the decision not to approve their accreditation as a data processor;
- The researcher/organisation disagrees with the decision not to approve trusted status for remote connection to the SRS setting;
- The researcher/organisation disputes the non-compliance;
- The researcher/organisation feels mitigating factors were not considered where a penalty was applied; and
- The researcher/organisation acknowledges non-compliance and that all mitigating factors have been considered, but disputes the penalty applied on the grounds of proportionality or consistency.

Further information on the appeals process in relation to suspected non-compliance, are set out in the Research Data Access and Accreditation: Non-compliance and Breaches Policy at Annex A. This includes the criteria to be considered for withdrawing a researcher's accreditation. This appeals process will be followed if a researcher or organisations wishes to appeal against a decision regarding their accreditation or status as a trusted organisation for remote connection to the SRS.

9. Roles and Responsibilities

Role	Responsible for:
Researcher	• Complying with the agreed terms and conditions of their access to ONS research data and/or research data held by ONS on behalf of other depositors • Ensuring confidentiality s is protected.

Role	Responsible for:
Senior Information Risk Officer (SIRO)	• Accountable and responsible for information risk across the organisation
Data Governance Committee	• Approve, monitor and review this policy and its application
Research Support and Data Access Team	• Monitoring the access to ONS research data by researchers to identify and address unsafe practices, providing guidance and delivering action to mitigate risks as necessary
Complaints Manager/Director of MDR	• Review and adjudicate any appeals where the appellant is not satisfied with the outcome.

10. Governance

Policy Owner:	Head of Research Support and Data Access (RSDA)
Policy Approval:	Data Governance Committee (DGC)
Compliance Monitoring:	Data Governance Committee (DGC)
Review and amendments	Research Support and Data Access (RSDA)

Appendix A

Contents

1. Introduction

This policy sets out our approach for dealing with non-compliance with the legal requirements and/or conditions of access under which access to the data was granted. It sets out the actions and underlying principles that will be adopted. The policy applies to all users of ONS data (whether hosted by ONS or other organisations on behalf of ONS) and research data hosted by ONS on behalf of other depositors (data owners), to ensure that the confidentiality of persons is protected. It forms part of the ONS Research Data Access and Accreditation Policy.

2. Background

The ONS Research Data Access and Accreditation Policy sets out the arrangements adopted by ONS to manage access to data for the purpose of statistical research that delivers a public benefit to the UK. The policy applies to all users of ONS research data and the wider research community as defined in 5.1 of the ONS Research Data Access and Accreditation Policy. This annex sets out our arrangements for dealing with non-compliance with that policy, or the terms and conditions for which access to data for research was granted, to ensure that confidentiality is protected.

3. Scope

The policy applies to the access to unpublished data for statistical research and the accreditation of researchers, projects and processors in relation to this access. It applies to:

- Access to ONS survey and administrative data managed by ONS or other organisations on behalf of ONS;
- Access to research data managed by ONS on behalf of other data owners in the Secure Research Service;
- Access to data owned by Public Authorities and made available to researchers through DEA and managed by ONS; and
- The accreditation of researchers, projects and processors for the access listed in 3.1, through the SRSA, DEA and other relevant legislation.

4. Objectives

The purpose of this policy is to ensure that:

- ONS takes transparent, consistent, proportionate and targeted action to deal with suspected breaches of lawful research data access and/or non-compliance with the conditions of data access (e.g. procedural breach), to help ensure confidentiality is protected; and
- Researchers/organisations are aware of: the sanctions that may be applied to them, the circumstances when they may be applied; and the process to appeal against ONS action should they wish.

5. Practices

Despite the rigorous arrangements in place to protect confidentiality, there is still the possibility for a breach to occur when an individual or organisation does not fulfill their responsibilities – willfully or unintentionally. This policy sets out our approach for dealing with non-compliance with the legal requirements and/or conditions of access under which access to the data was granted including any of those other circumstances set out in the Code of Practice and Accreditation Criteria for research powers in the Digital Economy Act 2017.

The types of breach that might result include:

- sharing the data/login details with persons who do not have lawful or authorised access, e.g. researchers not named on that project;
- sharing or publication of data that could result in the unlawful disclosure of information about a data subject (i.e. an individual or corporate body);
- accidental loss, destruction of or damage to personal data;
- Failure to have regard to the Code of Practice governing data sharing for research purposes;
- Deliberately recording information about a data subject and taking this information out of a safe setting;
- Failure to disclose information that could materially affect the accreditation process or has otherwise dishonestly completed the application form;
- Failure to adhere to the terms of any data access agreement between the data holding public authority and the researcher;
- Action that facilitates or negligently enables access to identifiable data by a non-accredited person; and
- failure to adequately manage the data to ensure confidentiality is protected

Any one of the breaches listed in paragraph 5.2 may result in a procedural breach or an unlawful disclosure of data and identification of a data subject. Since the enactment of SRSA and establishment of the ONS Approved researcher scheme, there has been no unlawful breaches. However, each year there are a number of procedural breaches by researchers which have resulted in further action and there remains a risk that any of these breaches could have resulted in something more serious. We will learn the lessons from each breach and provide further guidance and training to researchers as necessary.

The factors that may result in a data breach include:

- failure to comply with relevant Data Access Agreements or licence conditions;
- loss or theft of data or equipment on which the data is stored;
- inappropriate access controls allowing unauthorised use;
- unsafe settings;
- poor management of data security; and
- equipment failure

The risks that exist when there is a data breach could include:

- identification of persons and information about them;
- reputational damage to the data owner and/or processor;
- misuse of data; and
- loss of public confidence in granting access to research data

6. Investigation and Principles

6.1 We will investigate all suspected breaches to better understand the cause and prevent similar breaches from occurring. We undertake investigations to:

- gather information and establish the facts;
- identify the immediate and underlying causes and the lessons to be learnt, taking any remedial actions to address this and protect the data;
- prevent recurrence;
- identify breaches of the law;

- take appropriate and effective action; and
- learn from any trends or repeated incidents

6.2 We will contact the researcher to gather information about the suspected breach and assess the risk. We will maintain appropriate records of the investigation, including the methodology and findings. The decision will take account of the enforcement principles set out in paragraph 6.3. Specific factors which will be considered are set out in paragraph 6.5 as well the severity of the incident and the level of detail in the data (see figure 1 of the main Research Data Access and Accreditation Policy). We aim to complete investigations within 20 working days.

6.3 We apply the following **principles** when investigating breaches and in considering subsequent action:

- proportionality
- targeting of response
- consistency
- transparency
- accountability

6.4 **Proportionality** in how we apply the law and conditions of access to secure compliance is achieved by ensuring that our actions are proportionate to the risk.

6.5 We will, where necessary, take action against individuals and/or organisations. Where there has been a confirmed non-compliance, the following factors will be considered when determining any penalties applied:

- Whether the breach was self-reported;
- Whether the organisation/individual has robust data security arrangements and has taken action to stop reoccurrence such as refresher training, procedure updates etc.;
- Whether the researcher/organisation understands the implications of their behaviour;
- Whether there is a record of previous good conduct or non-compliance;
- The risk of disclosive/identification of an individual/business;
- Whether the non-compliance was deliberate or accidental;
- The willingness of the individual/organisation to assist in the investigation; and
- Whether it is an isolated incident or there is a risk of similar occurrences

6.6 **Targeting of Response:** investigative resources will be targeted where there is the greatest need and proportionate to the perceived risk. We will focus our compliance actively on the most serious risks and those who are responsible for, and best placed to control, those risks.

6.7 **Consistency:** we will adopt a consistent approach to enforcement of the policy and conditions of data access. Consistency of approach does not mean uniformity. It means taking a similar approach in similar circumstances to achieve compliance with the law and/or licence conditions. We will review the investigation action we take and the criteria we apply in making our decisions, to ensure they are consistent with our policy and those adopted by other data processors and/or controllers. Not all investigations will result in enforcement action.

6.8 Transparency is about being clear and unequivocal to our users about what they can expect from us and when. We will ensure that users of our research data are aware of the policy and help them to understand it. To promote transparency, we will do the following:

- Publish the policy on our website and make data users aware of its existence and content;
- When a suspected breach investigation is instigated, the researcher will be reminded of their responsibilities within the investigation process. They will be informed at which points in the process they will receive updates. They will be notified of their right to appeal and how to go about it;
- On completion of the investigation, where non-compliance has been identified, we will clearly and promptly explain the decision taken, the reason behind the decision and the actions required to achieve compliance. We will discuss reasonable timescales for corrective action and behaviour, and explain what will happen if there is a failure to comply;
- We will differentiate between the actions required to comply with the law and/or conditions of access, and advice given to achieve good practice;
- On an annual basis, we will publish a summary of all breaches of our policies & procedures, the actions taken in response, penalties imposed and lessons learned, on the ONS website; and
- We will review the policy from time to time, and in particular following any investigation, to ensure it remains relevant and accessible.

6.9 **Accountability:** We are accountable to users for the application and the outcomes of this policy, which will be published. This will help us to: ensure continuous improvement;

evaluate the policy; provide effective training and support; and promote public confidence. To promote accountability, we:

- have appropriate governance structures in place to ensure the outcomes of all investigations will be shared with the Senior Information Risk Owner (SIRO) and relevant Information Asset Owner (IAO). The SIRO is accountable and responsible for information risk across the organisation, supported by IAOs;
- be measured in the way we implement and enforce this policy. We will take required action to address any shortcomings in both the policy and our actions against it, and report on progress to implement these.

6.10 Where there is an ongoing risk to data confidentiality, then access will be suspended pending the outcome of the investigation. This would be done to protect data confidentiality and would not imply blame.

6.11 Where we host research data on behalf of another data owner, they may be involved in any enforcement decisions and actions. In a similar fashion, any breach of our data hosted by a third party, such as the UK Data Service, is likely to result in separate, but joined-up, investigations by both organisations.

6.12 It is anticipated that investigations and actions taken by other data providers (e.g. for data managed by us on their behalf) or data processors (for data managed on behalf of ONS or other data providers) will be carried out in a way that is consistent with this policy. This includes the accreditation of researchers, research projects and data processors facilitated by access to data for research under the Digital Economy Act 2017.

6.13 Where no breaches were found to have occurred, no formal action will be taken. In these circumstances, we may offer advice to individuals or organisations about data security arrangements.

6.14 Where we are of the opinion that a breach has occurred, we will consider a range of penalties which may result in the suspension of the researcher and/or organisation. The action taken will depend on the risk associated with the incident and consideration of the factors set out in paragraph 6.5. If a researcher takes prompt action to deal with a self-reported, unintentional non-compliance, we will take these factors into consideration when deciding possible action. The penalties will usually apply to the researcher or researchers who have breached. However, sanctions may also be applied to their organisations if there is a systematic failure of arrangements or behaviours to protect data confidentiality.

6.15 We may provide guidance and advice to researchers and/or organisations on safe practices regarding data security and protecting confidentiality. We may require improvements in the way security of data are managed as a condition for continued access. Failure to implement improvements may result in a temporary or permanent suspension.

Temporary Suspension

6.16 There are two types of temporary suspension:

- **Conditional Suspension –** access to our research data or data we are the controller for, will be temporarily suspended until required action has been completed, e.g. researcher re-training.
- **Fixed Period Suspension** of access for up to 12 months. Access to the research data by the researcher or organisation will be suspended for a period of up to 12 months. The timescale will depend on the findings of the investigation and the behaviour of the researcher. All temporary suspensions will require retraining before access is re-instated.

6.17 This suspension may also be applied in relation to the trusted status for an organisation (in relation to their remote connection to the SRS).

Permanent Suspension

6.18 An individual or organisation might be permanently banned from access to data. This will only be used where there has been a serious and/or intentional breach or repeated failings to protect data confidentiality.

6.19 This suspension may also be applied in relation to the trusted status for an organisation (in relation to their remote connection to the SRS).

6.20 We will inform the police/CPS for their consideration where there has been a serious breach of the applicable law. If they conclude that a breach of section 39 of the Statistics and Registration Service Act 2007 has been committed, this may result in prosecution by the Crown which could result in a prison sentence and/or a substantial fine, and criminal record.

7. Appeal Process

A researcher or organisation has a right to appeal if they disagree with the outcome of an investigation or if they believe we have not acted in accordance with this policy. Appeals against

legal action and any outcomes of such are not with-in the scope of this policy as that is dealt with by the CPS/Police. Examples of when a researcher might submit an appeal include:

- The researcher/organisation disputes the non-compliance;
- The researcher/organisation feels mitigating factors were not considered where a penalty was applied; and
- The researcher/organisation acknowledges non-compliance and that all mitigating factors have been considered, but disputes the penalty applied on the grounds of proportionality or consistency.

Any researcher or organisation subject to our investigation of a suspected breach, will be informed of the method of raising an appeal when the investigation is complete.

On receipt of the Appeal, we will undertake an **initial assessment,** by an officer independent of the initial investigation, within 10 working days. This will assess additional information provided by the appellant, including any information that we were not aware of when applying the penalty.

The initial assessment will endeavour to arrive at an outcome which is acceptable to both parties whilst remaining compliant with this Policy. An acceptable outcome could be achieved by either of the following means:

- Communication between parties leads to understanding that penalty was proportionate and therefore acceptable
- Communication between parties leads to agreement that the penalty disproportionate to the circumstances of the breach and that the penalty should be revised accordingly.

If the initial investigation does not achieve an outcome acceptable to both parties, we will appoint an independent ONS investigator to consider the appeal. The investigator will not have a connection with the specific case. We will contact the appellant with details of the investigator, timescales of the investigation, etc. The investigator may contact our staff and the appellant to request additional information if needed and/or seek clarification. The investigator will report on: their assessment of the 'breach' identified by us; their assessment of whether the penalty proposed was proportionate and consistent; and recommendations (e.g. to uphold or overturn our decision) for further action.

The appellant will be notified of the outcome of the investigation. If they are still dissatisfied with the outcome, they may escalate their concerns by submitting a formal complaint to the ONS Director of Methods, Data, Research (Sarah Henry) sarah.henry@ons.gov.uk, or in writing:

Director Methods, Data, Research
Office for National Statistics
Segensworth Road
Titchfield
Fareham
Hampshire.
PO15 5RR

8. Roles and Responsibilities

Role	Responsible for:
Researcher	• Complying with the agreed terms and conditions of their access to ONS research data and/or research data held by ONS on behalf of other depositors • Ensuring confidentiality s is protected.
Senior Information Risk Officer (SIRO)	• Accountable and responsible for information risk across the organisation
Data Governance Committee	• Approve, monitor and review this policy and its application
Research Support and Data Access Team	• Monitoring the access to ONS research data by researchers to identify and address unsafe practices, providing guidance and delivering action to mitigate risks as necessary
Complaints Manager	• Review and adjudicate any appeals where the appellant is not satisfied with the outcome.

9. Governance

Policy Owner:	Head of Research Support and Data Access (RSDA)
Policy Approval:	Data Governance Committee (DGC)
Compliance Monitoring:	Data Governance Committee (DGC)
Review and amendments	Research Support and Data Access (RSDA)

Appendix B: Glossary and Definition of Terms

Table 1 Definitions

Term	Definition
Breach	Either: a) non compliance with security policies and procedures, or b)
Controlled Data	Data which are identifiable under the SRSA and thus disclosive or potentially disclosive.
CPS	Crown Prosecution Service
Data Access Agreement (DAA)	An agreement setting out the terms and conditions of use of a data service and establishing the rights and responsibilities of the user of that service.
Data Owner	The ONS Manager responsible for the data
De-identified Data	Data that has had direct identifiers (such as name, address, National Insurance number) removed
Information Asset Owners (IAO)	ONS Manager responsible for managing the risk associated with the asset.
Personal Information	Information that relates to and identifies a particular individual (including a body corporate) taking into account other information derived from published sources
Research Data	Unpublished Data made available for research to organizations/individuals outside of ONS
Risk	In this policy, 'risk' (where the term is used alone) is a consideration of the likelihood and level of consequence (impact) of an actual or possible incident
Senior Information Risk Officer (SIRO)	Responsible for information risk across the organisation.
SRSA	The Statistics and Registration Service Act 2007