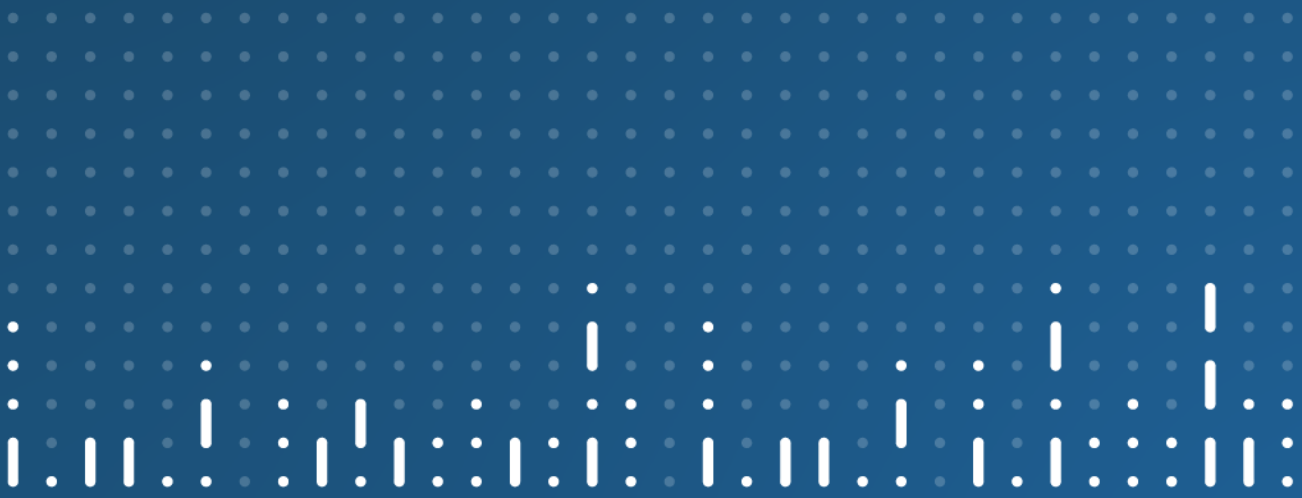
Office for National Statistics

ons.gov.uk

Managing identifiable data policy



Managing identifiable data policy

1. Scope

This policy applies to the use of identifiable data within the Office for National Statistics (ONS), to produce statistics and statistical research. It does not include operational data (sometimes called corporate data) such as information related to staff management, finance and other non-statistical information.

For the purposes of this policy, “identifiable data” means personal information as defined in the Statistics and Registration Service Act 2007 (SRSA). This means any information which can be used to identify an individual, a household, a public body or a business, either by itself or alongside other information. In this sense, it is broader than “personal data” as defined for the UK General Data Protection Regulation (UK GDPR) that only includes information relating to an individual.

The policy covers all personal information held by the ONS, whether this is collected as part of ONS data collection activities (for instance a survey) or by a third party and subsequently shared with the ONS.

The policy applies to:

- all ONS employees, including staff on fixed-term, temporary or permanent contract, staff on secondment, students and contractors
- external researchers in public sector bodies such as government departments and local authorities when they are given access to identifiable ONS data

The policy does not apply to:

- external researchers accessing data on the Secure Research Service (SRS), as this is not considered to be identifiable personal information, and whose access to unpublished data is covered by the SRS Research and Data Access Policy
- external researchers carrying out statistical research who would not be able to access identifiable data

2. Definition of personal information

Personal information is information that makes it possible to identify an individual (including a corporate body) from the information held, either alone or in combination with other information. Personal information might contain:

- direct identifiers, meaning that information exists in the dataset that directly identifies an individual
- indirect identifiers, meaning that information exists in the dataset that allows the identity of the individual to be inferred in combination with information in the dataset or information contained in other data sources
- distinctive characteristics that allow an individual to be identified, such as an extreme age or an unusual geographic location, for example, a person aged 120 years, or a shipbuilder in the Outer Hebrides

Personal information is most commonly used for linking (matching) datasets but on rare occasions it may be used for statistical research. Whenever personal information is used for research purposes, the Office for National Statistics (ONS) must be able to justify its use and demonstrate that it has considered and rejected other options.

3. Policy statement

The Office for National Statistics (ONS) collects and processes personal information in accordance with all relevant legislation, including the Statistics and Registration Service Act 2007 (SRSA) and the Digital Economy Act 2017 (DEA). In addition, personal data are covered by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

In all cases, any data collected can only be used for the production of official statistics and for approved statistical research.

There is an expectation that personal information is never published, and also that datasets approved for use in external research projects will be de-identified in line with the ONS de-identification policy. However, there are limited circumstances where personal information can be shared, subject to regulatory, legal and data protection restrictions, as described in ONS's Data Sharing Policy.

Datasets used by researchers are usually de-identified, but there may be very rare occasions where a researcher requests that some or all of the personal information is retained within the dataset. In these cases, the ONS must be satisfied that the personal information is being used safely, legally and ethically.

4. Policy detail

For the purposes of producing statistics or undertaking research, the Office for National Statistics (ONS) collects data from survey sources and non-survey sources. This includes third-party data that have already been obtained by other organisations. These data may contain personal information.

Official statistics

Data used in the production of official statistics are processed electronically by automated means. Any personal information within the datasets is used for linking and matching datasets and is never published. There is a clear separation of duties meaning that staff handling personal information are not actively involved in the production of statistics. ONS staff producing statistics do not have access to identified data.

As stated in the Data Classification and Handling Policy, everyone who works with the ONS has a duty of confidentiality and a responsibility to safeguard ONS information based on its classification. In line with the ONS de-identification policy, researchers accessing de-identified data should report concerns regarding quality to the team responsible for carrying out the de-identification.

Statistical research using de-identified data

Datasets used for statistical research are usually de-identified. The approach taken by the ONS for requests to include personal information in a research project is covered in the "Statistical research using personal information" section of this policy.

There is a clear separation of duties meaning that staff handling personal information for data processing (for example, ingestion, data engineering) are not actively involved in statistical research. ONS staff conducting statistical research do not have access to personal information.

As stated in the Data Classification and Handling Policy, everyone who works with the ONS has a duty of confidentiality and a responsibility to safeguard ONS information based on its classification. In line with the ONS de-identification policy, researchers accessing de-identified data should report concerns regarding quality to the team responsible for carrying out the de-identification. If research is conducted within a trusted research environment, staff must also report this to the team responsible for managing data access.

Datasets used for statistical research by external researchers are always de-identified before being approved for use. This is a requirement for data collected under the Digital Economy Act 2017 (DEA). If external researchers bring their own data into a trusted research environment, they are responsible for ensuring they are not identifiable. This is also verified by the teams responsible for managing data access in these environments.

Statistical research using identified data

Our data principles include protecting the confidentiality of individuals and using data multiple times to maximise its value. We need to find the right balance between these two principles. In maximising the value of data, there may be occasions where a researcher needs access to identified data in order to produce the proposed outputs for a research project. In these cases, the researcher may request that some or all of the personal information is retained within the dataset.

In all cases, the ONS must be satisfied that the use of personal information is justified and that it is being used safely, legally and ethically. Any access to personal information by researchers requires evidence listed in the following subsections.

Legislation and regulations

The data are being used in accordance with all relevant legislation and regulations. They are used within the original context and purpose for which they were collected (existing Memoranda of Understanding, Data Sharing Agreements) and if not, new approval has been obtained from the data provider. The data are also used in accordance with advice by Legal Services, where any advice is clearly recorded.

Assurance of the data request

The data requested must be proportionate to the expected benefits of the research that is proposed. The request must not exceed the requirements of the research project (data minimisation).

Data security considerations

The data must be stored in a secure environment with controlled access. The duration of the data use must be stated so that access to the data can be time-bound, with access being removed when no longer needed.

Data protection

If personal data are involved, ensure compliance with the Data Protection Policy, including undertaking a Data Protection Impact Assessment (DPIA) if appropriate.

Ethical use of the data

The Data Ethics Policy must be adhered to and the Ethical Principles upheld. The researcher must use the Ethics Self-Assessment Tool and share the results with the UK Statistics Authority's Centre for Applied Data Ethics. Following submission of the self-assessment, any advice provided by the Centre for Applied Data Ethics or by the National Statistician's Data Ethics Advisory Committee must be followed.

Adherence to relevant policies

Researchers must state the policies that apply and ensure they are followed. They must escalate to the appropriate level for approvals that are required to manage the risk associated with this use of identified information. Risk assessment is not a one-off task but should be carried out at all stages of the data life cycle.

5. Roles and responsibilities

National Statistician

Responsible for the Office for National Statistics' (ONS's) compliance with data protection legislation.
Accountable to Parliament.

Data Protection Officer (DPO)

Responsible for monitoring compliance with and providing advice and guidance on data protection.
Accountable to the National Statistician.

Data Protection Compliance and Audit Team (DPCA)

Responsible for monitoring and auditing the ONS's compliance with data protection legislation.
Accountable to the Data Protection Officer (DPO).

Chief Security Officer (CSO)

Responsible for ensuring the ONS's services using personal data are compliant with data legislation.
Accountable to the National Statistician.

Security and Information Management Team (SaIM)

Responsible for oversight of all data management activities.
Accountable to the Chief Security Officer (CSO).

Security Compliance and Audit Team

Responsible for monitoring and auditing the ONS's compliance with security policies.
Accountable to the Chief Security Officer (CSO).

Legal Services

Responsible for providing support to the whole of the UK Statistics Authority and the ONS.
Accountable to the National Statistician.

Senior Information Risk Officer (SIRO)

Responsible for information risk across the organisation.
Accountable to the National Statistician.

National Statistician's Data Ethics Advisory Committee (NSDEC)

Responsible (in the scope of this policy) for providing ethical approval for researchers who wish to use government data for research and statistics that serve the public good.
Accountable to the UK Statistics Authority Board.

UK Statistics Authority Centre for Applied Data Ethics

Responsible for providing oversight of the ethics self-assessment tool, providing advice and guidance to researchers, reviewing the self-assessments, agreeing actions to mitigate risks and submitting projects to NSDEC when risks cannot be mitigated.
Accountable to the National Statistician's Data Ethics Advisory Committee (NSDEC).

Information Asset Owner

Responsible for approving access to the data and its use for the research.
Accountable to the director of the business area that owns the information.

Data Governance Committee (DGC)

Responsible for approving, monitoring and reviewing the policy and its application.
Accountable to the National Statistics Executive Group (NSEG).

Secure Research Service (SRS) Team

Responsible for complying with and delivering policy requirements in the SRS.
Accountable to the Data Governance Committee (DGC) and Data Owners.

Researchers

Responsible for complying with the policy and completing all documentation.
Accountable to the ONS and Data Owners.