National Energy Efficiency Data-Framework (NEED): Accessing property level data

May 2020

This document sets out four routes for individuals or organisations outside of the Department for Business, Energy & Industrial Strategy (BEIS) to access the NEED property level data. Further information on how BEIS manages the NEED data is set out in the Privacy Impact Assessment[1].

The NEED data is made up of various components, each of which is acquired under different legislation or agreements. The suppliers of each component are shown in Table 1 below. Because each component must abide by different rules (including those on further sharing) not all components of NEED are available via every route.

Table 1: The data sources used in the production of the NEED data

Data	Supplier
Meter level electricity consumption	Electricity suppliers and data aggregators
Meter level gas consumption	Xoserve
Property characteristics	Valuation Office Agency (VOA)
Household characteristics	Experian
Installations of energy efficiency measures (e.g. Energy Company Obligation, Feed in Tariff)	Ofgem
Installations of new boilers	Gas Safe register

Queries about this document are welcome and should sent to: energyefficiency.stats@beis.gov.uk.

[1] https://www.gov.uk/government/publications/national-energy-efficiency-data-framework-privacy-impact-assessment-2019

Anonymised dataset

The latest NEED anonymised dataset was made openly available in December 2019. This includes two tables, one small enough for spreadsheet software and a larger table for more in-depth analysis. Both are samples of the full NEED data.

NEED data accessible:	Gas and electricity meter consumption, property characteristics, installation of energy efficiency measures, property council tax band, conservatory flag
Data coverage:	England and Wales
Key information:	Openly available; unable to link to other datasets

As the anonymised dataset is the easiest route to accessing the NEED data, this is the recommended choice wherever possible.

The anonymised dataset with accompanying metadata can be found at: www.gov.uk/government/collections/national-energy-efficiency-data-need-framework#record-level-data

Secure research service (SRS)

The SRS, run by the Office for National Statistics (ONS), provides secure access to de-identified public sector data for research. The consumption data from NEED is just one dataset among many which researchers can access.

To use the SRS researchers must complete an accreditation process, before applying to carry out a specific project. Where justified by the project, multiple property level datasets can be linked by ONS staff and used by the researcher.

NEED data accessible:	Gas and electricity meter consumption
Data coverage:	England, Scotland and Wales
Key information:	Allows linking to a wealth of other data in the SRS (e.g. educational outcomes of residents)

There is no charge to apply for or use the SRS.

More information on the SRS, alongside the full SRS Data Catalogue, can be found at: www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/approvedresearcherscheme

Undertaking work on behalf of BEIS

a) Contracted work

In certain cases BEIS contracts third parties to act on its behalf. These contractors are given access to select NEED data for specifically approved projects.

Contractors are acting on behalf of BEIS. This means that if the NEED data is required to fulfil the contract, it can be shared with named individuals in the contracted organisation subject to meeting secure data handling and other terms and conditions.

All projects carried out by BEIS contractors using NEED data are governed by specific contracts. Only the minimum data required to deliver the project outcomes are provided to third parties.

NEED data accessible:	**All NEED data**
Data coverage:	England, Scotland and Wales
Key information:	Requires legal documentation (e.g. data sharing agreement). The data must be held, accessed and processed in a manner which meets the security requirements of the NEED data. This includes the data be restricted to the minimum number of staff required and stored on a secure server (see Appendix A of this document).

b) Secondments

This route is only used if other approaches are not feasible and if the work has significant public benefit. Applicants will have to demonstrate such a public benefit to justify the secondment.

Under this route the researcher is treated as part of the NEED team in BEIS for the duration of the project but remain employed in their existing role, with all salary costs etc continuing to be met by their employer. However they will have access to BEIS IT equipment, data and technical support allowing them to access the full NEED dataset. The researcher's employer can be in any sector.

NEED data accessible:	All NEED data
Data coverage:	England, Scotland and Wales
Key information:	The researcher becomes part of the NEED team for the duration of the project

BEIS will fund only the necessary Baseline Security Clearance and supply IT equipment. Desk space may also be provided for at least 1 day per week, and support from the NEED team to understand the tools and data available.

Security clearance must be completed prior to starting.

The secondment can be from 1 week to 3 months.

From an HR perspective the secondment would be treated as a work experience placement.

Applications for this route should be sent as an email or document to: energyefficiency.stats@beis.gov.uk. Applications should include:

- The aims of the proposed project
- Why the project is in the public interest, including expected impacts of the project
- How the project will be carried out
- How the results will be used and communicated

For initial enquiries, please contact the NEED team at the above email address.

Appendix A: Technical requirements for contractors to hold NEED data

For any NEED data to be shared with a contractor, BEIS must first be certain that the IT platform used to store the data will not be compromised. This is essential, as NEED data is considered personal sensitive.

The data protection requirements and procedures in (a) below must be met. Also required is an adequate explanation of how each of the IT security principles set out in (b) below are met by the IT system used. Applicants should be able to obtain this information from their IT system provider.

a) Data protection requirements and procedures

Data to be held only on a secure system physically based in the EEA and/or UK including any backup or redundant data.

All data to be kept on the secure server in a restricted access container or folder, with access only granted to named staff for whom access is necessary to complete the work specified in the contract and as detailed in the Data Sharing Agreement.

All data to be securely deleted from the contractor's IT system as soon as it is no longer needed or used under the terms of the contract, or when instructed to do so by BEIS.

All data to remain in the contractor's IT system and not be transferred elsewhere without written BEIS consent.

The contractor will not share any output generated from this data with any third party without BEIS consent.

The contractor will use the data solely for the purposes specified in the contract or such other purpose as BEIS may agree in writing, and not further process the data. This applies to all granular and aggregate outputs generated during the contract.

b) IT security principles

1. Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another.

2. Governance framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it.

3. Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

4. Personnel security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

5. Identity and authentication

All access to service interfaces should be constrained to authenticated and authorised individuals.

6. External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended.

7. Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

8. Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

This publication is available from: https://www.gov.uk/government/collections/national-energy-efficiency-data-need-framework

If you need a version of this document in a more accessible format, please email energyefficiency.stats@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.