CODE OF PRACTICE

Secure Data Service members

As a community, we aim to get the most research value from existing data while protecting the privacy of respondents. For this reason, we subscribe to a common code that guides us in our everyday practices.

We all agree

- to not share data or outputs with anyone who is not authorised to access them – whether verbally, written or onscreen
- to not disclose personal logon details to anyone else
- to ensure that access is available only to those who need it
- to not compromise any personal information
- to report incidents of any unauthorised access, processing or disclosure of personal information
- to understand what constitutes a breach and the resulting consequences
- to follow recommended security procedures
- to use up-to-date anti-virus software
- to inform one another of any errors discovered in the data
- to make syntax available within the research community

Users agree

- to become trusted researchers by abiding by our core agreements:
  - the declaration for Approved/Accredited Researchers
  - User Agreement
  - Microdata Handling and Security: Guide to Good Practice
- to use the data only for an approved purpose and duration
- to not link the data to any other source of data except where explicitly approved
- to not remove (or attempt to remove) any personal information
- to not remove or share any outputs before they're checked for Statistical Disclosure Control and released by the Secure Data Service
- to share research publications and case studies with the Service
- to use the correct form of citation and acknowledgement in any publication
- to follow the guidance outlined in Secure Data Service training
- to provide the Service with code for creating derived data

The Service agrees

- to become a trusted resource by abiding by our Service Promise
- to provide a timely, helpful and friendly service
- to liaise with key stakeholders and data owners to enable access to data
- to acquire, process and catalogue data
- to handle and store data securely, ensuring physical and technical data security
- to be compliant with the international ISO 27001 standard
- to train Service staff in data handling and security
- to run baseline security checks on Service staff
- to require staff to sign a non-disclosure agreement
- to act on reported and discovered breaches
- to provide training and training materials
- to monitor and support use of the Secure Data Service system
- to remove access to data at project expiry
- to store syntax files for researchers
- to follow agreed Statistical Disclosure Control standards for output checking

Data owners agree

- to provide good quality data that's clearly labelled and well documented
- to assist the Service with queries about the data
- to investigate errors or omissions in the data
- to remove direct identifiers from the data
- to support use of the data
- to offer data at an appropriate level of access

SECURE DATA SERVICE
UK DATA ARCHIVE
UNIVERSITY OF ESSEX
WIVENHOE PARK
COLCHESTER
ESSEX CO4 3SQ

Service provided by the UK Data Archive

In partnership with the Economic and Social Data Service

Funded by the Economic and Social Research Council