Code of practice

Members of UK Data Service - secure access

15/10/18

Version No. 03.00

Table of Contents

An important message

As a community, we aim to get the most research value from existing data whilst 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
- not disclose personal logon details to anyone else
- ensure that access is available only to those who need it
- not compromise any personal information
- report incidents of any unauthorised access, processing or disclosure of personal information
- understand what constitutes a breach and the resulting consequences
- follow published best practice guidelines
- use up-to-date anti-virus software
- inform one another of any errors discovered in the data
- make syntax available within the research community
- provide clear information on our websites and printed materials that helps our users and data owners find what they need
- provide personal guidance when needed, available via an online help desk and a telephone help line.

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
- not remove or share any outputs before they’re checked for Statistical Disclosure Control and released by Secure Access
- share research publications and case studies with the service

- use the correct form of citation and acknowledgement in any publication
- follow the guidance outlined in Secure Access training
- provide the service with code for creating derived data.

The service agrees to:

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

Data owners agree to:

- provide good quality data that's clearly labelled and well documented
- assist Secure Access 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.

www.ukdataservice.ac.uk

help@ukdataservice.ac.uk

+44 (0) 1206 872143

We are supported by the University of Essex, the University of Manchester, UKRI through the Economic and Social Research Council, and Jisc.