SHARING DATA ETHICALLY AND SECURELY: A NOTE FOR UNDERSTANDING SOCIETY DATA USERS (September 2023)

Data sharing is fast becoming a new paradigm in research across all disciplines, according to the UK Data Service (UKDS). This can provide benefits for social and economic research, and to individual researchers, institutions, funders and others. The Information Commissioner also produces higher level guidance on data sharing to provide organisations the confidence to share data in a fair, safe and transparent way in a changing landscape.

This note has been prepared for **individual researchers** (not organisations) in response to queries about whether Understanding Society data could be shared, and how to do this ethically and securely, when researchers are working together in teams which are spread *across* institutional boundaries. While it does not directly cover information about sharing data between researchers *within* institutions, similar due diligence and security measures need to be applied.

It is very important that data management protocols are correctly followed when working in cross-institutional research teams.

Ownership for data management and security

The UKDS provides an archive for different types of the data, with three levels access, each with their own security protocols. These are Open Data, Safeguarded Data, and Controlled Data.

This note *only relates to Understanding Society Safeguarded Data*. Use of Safeguarded Data is subject to the UKDS End User Licence (EUL) Agreement. For anything else please contact the UK Data Service directly.

UKDS Access Categories

Open Data: These data are not personal data, available for re-use under Open Licences and have very few restrictions. An UKDS account is not required to download these data.

Safeguarded Data: These data are effectively anonymised data where the data owner considers there to be residual risk of disclosure. The safeguards to mitigate this residual risk include knowing who is using the data and for what purpose.

Controlled data: These data are classified as personal data and therefore need to be most secure. They contain information that could identify individuals and only available to researchers for specific usage and projects that have been individually approved by the data owners, to be used within the UKDS SecureLab only.

The EUL is an agreement between the UK Data Service (UKDS) and *the individual researcher* that ensures data is used ethically. An essential condition of the EUL is that you comply with UKDS' security requirements. This remains the responsibility of the registered user *individually on behalf of their organisation*. All Safeguarded Data must be stored under conditions that meet the undertakings given in the End User Licence Agreement. In particular see the UKDS Research data handling and security guide for users - Section 4 on data storage and security and Section 8 for organisational responsibilities.

By far the easiest way to manage the issue of sharing data is to share code - not datasets. But if you need to share the underlying dataset from your research project, perhaps because members of your research team are using different statistical packages, please ensure that what you want to do complies with the UKDS requirements.

Based on advice received from UKDS, you will need to comply with **BOTH** the following steps if you need to share data between UKDS registered research team members who work in different institutions.

Step 1: One team member adds others to a project with the UKDS

The central requirement is that you cannot share data with other registered users working on *different* research projects – irrespective of what type of secure platform is used to do it. Usually, when becoming a registered user with the UKDS each participant will have individually signed-up and specified what research project they want to undertake using Understanding Society Safeguarded Data, e.g. usually Study Number 6614.

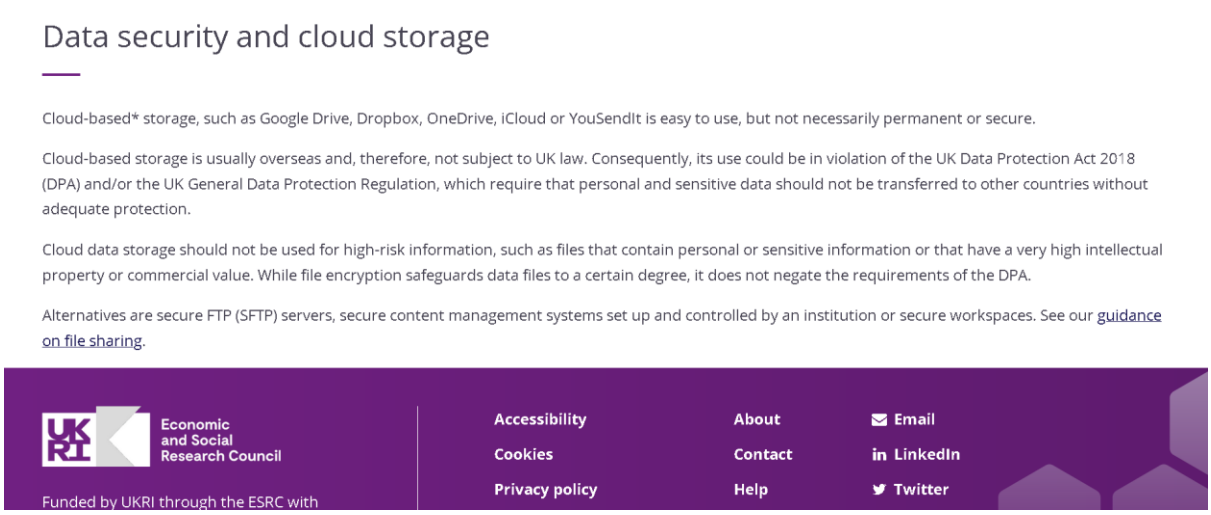
Where a multi-disciplinary team is being established to undertake research, one of the research team members can create a research project in their UKDS account, add the SN6614 dataset to this project, and assign other research team members as project members. One dataset can be attached to multiple projects. This step is important because the data owners need to sign off both on the *person using the data* and the *purpose for which the data is being used*. This is an essential requirement before any Safeguarded Data can be shared.

A date for project completion also needs to be specified, which you need to agree with the other team members, and all data shared will need to be deleted/destroyed once the project is completed. Please note that if the project continues after the proposed end date you can request UKDS to extend the end date.

Step 2: Safely sharing a dataset

For collaborative research projects, UKDS has provided guidance on various options for setting up a collaborative research environment and how to securely share files. You will need to ensure that the institutional platform you are planning to use is a secure platform. This is an essential condition of the EUL requirement. Please see: https://ukdataservice.ac.uk/learning-hub/research-data-management/store-your-data/security/ .

There is no list of which platforms are defined as secure or unsecure, but the UKDS guidance does set out the advantages and disadvantages of the various options.



More specifically:

a. the onus of what software or platform to use rests with your institution. Most organisations will have their own Information Security policies so if in doubt please consult the relevant person in your organisation to check what software they recommend as being secure for transferring files. E-mails and other communications software such as SLACK are NOT secure.

b. given the terms and conditions of the EUL that apply to the use of Safeguarded Data, encryption software approved and provided by your institution could be a good solution for transferring data. Encryption software such as VeraCrypt, BitLocker, Axcrypt, FileVault2, Time Machine, etc. can be used. There are Youtube tutorials available on these software.

c. cloud-based storage, such as Google Drive, Dropbox, OneDrive, iCloud are easy to use, *but not necessarily permanent or secure*. In general cloud storage without personal authentication and password protection are not secure.

UKDS recently ran a short data management and data sharing course in April 2023. The event recording is now available on UKDS YouTube channel: https://www.youtube.com/watch?v=ud7AcyLWoJE.

Please consult the UKDS User Support Service directly for further information or clarification. There is a Help Desk form you will need to submit: https://beta.ukdataservice.ac.uk/help.

Internal Management
Review data: September 2023
Version: v2.1
Owner: IT and Security Manager, ISER