



Economic and Social Data Service

Guide to good practice:
micro data handling and security

ESDS Access and Preservation

Author: Karen Dennison
Version: 2.0
Date: 24 April 2008

Contents

Introduction.....	3
1. Licence framework	3
1.1 End User Licence	3
1.2 Special conditions	3
2. Accessing data	4
2.1 Re-use of data	4
2.2 Research projects and teams	4
2.3 Teaching purposes.....	4
2.4 Security	4
3. Data storage security	4
3.1 End User Licence	4
3.2 Special Licence.....	5
3.3 Passwords and pass-phrases	5
3.4 Audit of confidentiality and security procedures	6
4. Statistical disclosure.....	6
4.1 Direct disclosure.....	6
4.2 Indirect disclosure	6
5. Reporting publications	7
6. When research is complete	7
6.1 Guidelines on destroying data	7
7. Institutional responsibilities	8
7.1 Special Licence responsibilities	8
8. Breach procedures	8
9. Help and feedback	9

Introduction

This guide is for users of micro data obtained from the UK Data Archive (UKDA), a service provider for the Economic and Social Data Service (ESDS). In particular, all users who obtain Special Licence data, including data that require Accreditation as an Approved Researcher, are required to read it under the terms of access.

1. Licence framework

The UKDA is the guardian of data for the data owners. The conditions under which data may be accessed are specified under licence with the data owners. These conditions include providing the data only to users who have registered with the ESDS and agreed to an End User Licence (EUL). Researchers accessing the data have responsibilities to preserve data confidentiality and to observe the ethical and legal obligations pertaining to the data. In particular, researchers must maintain the commitments made to survey respondents to preserve the confidentiality of the data provided.

1.1 End User Licence data

Use of the data is governed by a legally-binding EUL which forms part of the registration process. Each individual who requires access to data has to register and will need an Athens login. Users outside UK higher or further education who have no way of obtaining an Athens login can apply to the UKDA.

Under the terms of the EUL, users agree:

- not to use the data for any commercial purpose (except with prior permission/under an appropriate commercial licence agreement);
- to preserve the confidentiality of, and not attempt to identify, individuals, households or organisations in the data;
- to use the recommended methods of citation and acknowledgement in publications;
- to supply the bibliographic details of any published work based on the data collections;
- to ensure that the means of access to the data (such as passwords) are kept secure and not disclosed to anyone else;
- to abide by any further 'special conditions'.

1.2 Special conditions

Additional legally-binding conditions to those of the EUL may be specified by the data owners for particular datasets. Where data pose a higher risk of disclosure, special conditions may take the form of a Special Licence that requires the completion of an additional application form, the signature(s) of the researcher(s), and the explicit permission of the data owners to release the data to the researcher(s). Access to Special Licence data may be restricted to certain users (for example, to UK applicants only).

The coming into force of the Statistics and Registration Service Act on 1 April 2008 brings to an end the arrangements that have been in operation since September 2005 for access to ONS Special Licence data. Access to such data via the UKDA is available through a new legal framework set out in the Act. Any registered user wanting to access data previously available through a Special Licence will have to be accredited by the UK Statistics Authority as an Approved Researcher. To apply for accreditation a user will complete (i) forms that will require evidence that he/she is a fit and proper person and details about the purpose of the research (ii) an online order for the data and (iii) a signed declaration that he/she understands the confidentiality obligations owed to those data including its physical security.

2. Accessing data

Data can only be accessed under certain conditions:

- under the EUL, data can only be accessed by registered users;
- data supplied under special conditions can only be accessed by those who have accepted these conditions;
- Special Licence data can only be accessed by approved individuals for a specified usage.

2.1 Re-use of data

To re-use data already supplied, but for a different purpose, it is necessary to re-apply for access. For example, if depositor permission is required, this will need to be obtained again.

2.2 Research projects and teams

Users are required to register all usages of data, and to add other users working on the same usage to the usage details in their UKDA online account. Each usage is given a period of access that cannot exceed two years for EUL data and three years for Special Licence data. Users should contact the help desk to extend the expiry date of a project.

Where a researcher joins a research team that is using Special Licence data:

- the new researcher must place an online order for the data;
- permission must be sought and gained before the new researcher can access the data;
- the UKDA will provide advice on the process to be followed.

2.3 Teaching purposes

When using data for teaching all students must be registered or have signed an access agreement for teaching, which should be returned to the UKDA.

Special Licence data cannot be used for teaching.

2.4 Security

Passwords and pass-phrases should never be disclosed to anyone else. Data should not be left on a computer that might enable unauthorised access.

3. Data storage security

3.1 End User Licence data

All data provided by the UKDA needs to be stored under conditions that meet the undertakings given in the EUL (see section 7 for institutional responsibilities):

- access to PCs on which data are held should require personal authentication (secure username and password/pass-phrase);
- if data are placed in a shared directory or on a Local Area Network (LAN), access should only be available, via personal authentication, to those permitted to use the data;
- means of access to the data (such as passwords or pass-phrases) should be kept secure;

- data must be stored securely with data on portable media (e.g. a back-up on CD) protected using a secure password/pass-phrase;
- users should be aware of, and follow, any additional information security guidelines provided by their institution/organisation.

3.2 Special Licence data

Special Licence data should additionally:

- be protected, where possible, using pass-phrases instead of passwords;
- be stored in physically secure conditions (e.g. any portable or printed copies should be stored in a locked cabinet with restricted access);
- be stored on a PC in a room which is NOT accessible to the general public;
- be stored on a PC in a locked office when unattended;
- be protected by a screen-saver with an interval of five minutes and that requires a secure password/pass-phrase to unlock it;
- only be accessed, in an institutional setting, via a stand-alone PC or a closely controlled LAN with restricted access - data must not be accessed at a private residence;
- must not have live Internet links while the data are unencrypted on the machine unless access is through a secure organisational provider, such as JANET: (If there is any uncertainty as to whether an organisational provider is 'secure' users should contact the help desk with details of the system in place.)
 - stand-alone PCs and LANs, which have Internet access via broadband (and not through a secure organisational provider e.g. JANET) must be disconnected from the Internet and the broadband cable must be physically disconnected from the PC;
 - stand-alone PCs and LANs, which have Internet access via dial-up telephone connection (and not through a secure organisational provider e.g. JANET), must not have live internet links while the data are unencrypted on the machine;
- be accessed on a site which has security standards that meet the guidelines in this guide;
- be auditable;
- be accessed at a site within the UK as Special Licence data will not be provided to licence holders who are sited at, and thus would intend to access data, at an institution that is not within the UK;
- be deleted upon project completion:
 - this must be confirmed by the licence holder;
 - copies of data (including derived datasets) must be deleted from all PCs used;
 - any printed or electronic copies, including back-ups, temporary or intermediate files, must be destroyed;
 - any portable copies (e.g. CDs) must be destroyed or returned to the UKDA;
 - Section 6.1 has detailed guidelines.

3.3 Passwords and pass-phrases

Pass-phrases differ from passwords in format and in length. Pass-phrases are usually much longer - up to 100 characters or more and contain spaces. The greater length and format of pass-phrases makes them more secure.

A password should contain a combination of at least 8 alphanumeric and symbolic characters. Quotes should not be used as pass-phrase characters.

Passwords and pass-phrases should:

- not be disclosed to anyone else;
- not be written down;
- be changed at least every three months;
- not be easily guessable;

3.4 Audit of confidentiality and security procedures

The depositor of Special Licence data may reserve the right to conduct an onsite audit of the licence holder's confidentiality and security procedures and practices, or to require a report of such an audit. For the purpose of conducting an audit, the depositor may reserve the right of entry to the premises where the data are stored and processed. (Also see section 7.1 below).

4. Statistical disclosure

4.1 Direct disclosure

The EUL requires an undertaking not to attempt to identify any individual, household or organisation or claim to have done so. Where EUL data are matched with external data sources this must not be for the purposes of identification.

For Special Licence data, it is forbidden to attempt to match individual, household, or organisation records to any other data, including data from other Special Licence data series, at the level of individual, household or organisation. Only area-level descriptors or other group-level classifications may be matched for analysis purposes.

4.2 Indirect disclosure

Outputs from Special Licence data must be subjected to disclosure control. The guidance below is general advice but users should also refer to the full details of the procedures to be used in the Government Statistical Service (GSS) guidance available from the [Office for National Statistics Access Arrangements web page](#).

Tables that contain very small numbers in some cells may be disclosive. Tables should not report numbers or percentages in cells based on only one or two cases. Cells based on one or two cases should be combined with other cells or, where this is not appropriate, reported as zero per cent.

Tables and other outputs must not be published in a form where the level of geography would threaten the confidentiality of the data. To guarantee safety, outputs from Special Licence data should not be published if the geography is lower than UK Government Office Region (GOR).

If there is a requirement to publish outputs from Special Licence data with a lower level of geography i.e. between GOR and local authority, then the licence holder must consider whether there is a risk of disclosure. Where there is any doubt, the licence holder must contact the help desk to gain confirmation of the confidentiality of any outputs for publication with geography below GOR.

No outputs may be published with a geography below local authority.

Although most outputs from models or other statistical analysis will not be disclosive, care should be taken to ensure that individuals, households or organisations cannot be identified. In particular, results based on very small numbers should be avoided. Any output that refers to unit records, e.g. a maximum or minimum value, should be avoided. Models should not report actual values for residuals.

Graphical outputs should be based on non-disclosive data. Particular care should be taken not to report extreme outliers. Graphical outputs should respect all the rules specified in the GSS Disclosure Control Policy.

5. Reporting publications

All users of data are required to report publications arising from their research to the UKDA. It is good practice to inform the UKDA of any publications at the time of publication.

UKDA will provide annual reports to ONS on publications arising from the use of ONS Special Licence data.

ONS reserves the right to ask to see drafts of publications based on ONS Special Licence data for the purpose of commenting regarding compliance with the conditions for disclosure protection. If this condition is imposed, users will be notified when their application is processed.

6. When research is complete

It is recommended that researchers always retain a well-documented copy of the syntax used to prepare a paper or report. Derived data should be offered for deposit at the UKDA.

When a project has been completed it is good practice for researchers to remove all copies of the data, including derived datasets, back-ups, paper copies, portable copies (including CDs), and all electronic copies from every PC used.

Where Special Licence derived data are offered for deposit at the UKDA, UKDA will maintain the data on behalf of the user in a secure area for a five-year period. To re-access the data, the researcher should contact the UKDA .

It is essential that all copies of Special Licence data held by researchers are destroyed or, where held on portable media, returned to the UKDA at the end of the specified time period.

6.1 Guidelines on destroying data

The following are guidelines for destroying data:

- data should be deleted from the system on which it has been stored using a secure erasure programme, such as Disk Sanitizer (www.east-tec.com/eraser/index.htm) or similar - which repeatedly overwrites files a number of times, until such time as the original data could not be retrieved forensically;
- the recycle/trash bin should be emptied, preferably to be immediately followed by running a secure erasure programme to erase the unused areas of the disk;
- CDs and portable media should be returned to the UKDA or cut into many pieces or shredded using a disk shredder and then securely disposed of;
- backup tapes should either be completely overwritten and degaussed (demagnetised) before being re-used or disposed of;
- paper copies should be destroyed by shredding, preferably using a cross-cut shredder;
- before the PC leaves the possession of the organisation (for destruction or second hand sale, etc.) the hard disk should be completely erased using a secure erasure programme;

- destruction of Special Licence data must be confirmed to the UKDA by the licence holder.

7. Institutional responsibilities

Institutes of UK higher or further education (HE/FE), are bound by JANET policies (www.ja.net/services/publications/policy/security-policy.pdf), including the JANET Security Policy that places responsibilities on every person and organisation involved in the use or operation of JANET to protect the network against security breaches. UK HE/FE should also follow JISC guidance on information security, including handling information legally (www.jisc.ac.uk/uploaded_documents/ACF63.pdf).

There is a requirement that all central government departments must meet internationally recognised information and security management standards (e.g. ISO/IEC 17799 and BS 7799) for their systems. Local authorities are also obliged, by 2005, to comply with the BS 7799 security standard as part of their Implementing Electronic Government (IEG) requirements.

7.1 Special Licence data

Where access to Special Licence data requires an institutional signature:

- in Universities, the application should be signed by the Head of Department or School, Head of Research Centre, or the chair of the University Ethics Committee;
- in Government departments, or local authorities, the licence should be signed by the statistician with responsibility to represent the organisation or to enter it into a contractual relationship;
- in all cases an institution is required to accept legal responsibility for the user.

For a user accessing ONS Special Licence data through the Approved Researcher mechanism, it is the user's responsibility to ensure that they can store and access the data in a suitably secure physical and electronic environment.

Users of Special Licence data undertake to allow the depositor access to the premises where the data are stored and accessed for the purpose of conducting an audit, without notice and at any reasonable time. (Also see Section 3.4).

Access to ONS Special Licence data may require the user to provide the contact details of a senior member of staff at their institution who can vouch for their suitability for access to the data. The UKDA and ONS reserve the right to contact the senior member of staff to ask for a reference.

8. Breach procedures

The licence holder is required to report promptly a breach of any of the terms of the EUL, including the terms of any data supplied under special conditions. Failure to disclose details of a breach constitutes a breach of the licence.

Breach of the terms of the EUL, including any special conditions, may result in the following actions:

- immediate termination of access to all services provided by UKDA and ESDS either permanently or temporarily;
- legal action being taken against the individual who has breached the terms of the EUL;
- withdrawal of access, via Athens, to all UKDA and ESDS services either permanently or temporarily to the licence holder's institution.

Additionally, any breach in the terms of access for Special Licence data:

- will result in the immediate termination of the licence holder's access to the data, the termination of the licence and the prohibition of any further access to data supplied under the Special Licence;

- may result in sanctions being sought against the licence holder by the data owner;
- for ONS Special Licence data, under the Statistics and Registration Services Act 2007, will incur penalties as specified in S39 of the Act. This may include a fine and/or imprisonment.

9. Help and feedback

This guide will be regularly updated. For further advice on any of the issues raised, or to provide suggestions or comments, contact the help desk:

- email: help@esds.ac.uk
- telephone: +44 (0) 1206 872143



Economic and Social Data Service

ESDS Access and Preservation
Economic and Social Data Service
UK Data Archive
University of Essex
Wivenhoe Park
Colchester
Essex CO4 3SQ

Email: help@esds.ac.uk
Tel: +44 (0)1206 872143
Fax: +44 (0)1206 872003
www.esds.ac.uk