DSS Longitudinal Survey Handbook for Organisations and their Data Manager
About this Handbook

You should read this handbook if you are an Organisational Delegate or a Data Manager or considering undertaking the role of Data Manager for your organisation. This handbook will outline the role and responsibilities of the organisation and Data Manager plus will inform you on who can apply for access to any of the HILDA (Household, Income and Labour Dynamics in Australia), LSAC (Longitudinal Study of Australian Children) and LSIC (Longitudinal Study of Indigenous Children) datasets (‘the datasets’).

Roles and Responsibilities of the Organisation

The Organisational Deed of Licence or MOU is signed by the Organisational Delegate. The Organisational Delegate will be a person in a senior position within the organisation who has the delegation to commit the organisation to the terms and conditions in the Organisational Deed of Licence or MOU. In particular, for the Organisational Deed of licence these include but are not limited to, indemnity and intellectual property provisions and in the case of the MOU provisions relating to reimbursement of costs and management of intellectual property. For the purpose of these arrangements, and with agreement from DSS, organisational licensing arrangements may be entered into with a subdivision of an organisation where the organisation as a whole does not wish to enter into an agreement. This may result in one organisation having several organisational licensing agreements. For example, individual schools or faculties may sign organisational licences rather than the university as a whole. The Organisational Delegate agrees that the organisation will:

- Accept responsibility for any other HILDA, LSAC or LSIC datasets to which an Authorised User has previously been given access under an individual deed when that Authorised User is granted access to one of the Datasets under organisational licensing arrangements. The terms and conditions of any and all individual deeds previously signed by an Authorised User will be superseded by the Organisational Deed of Licence, MOU and the Deed of Confidentiality;
- Provide an officer to undertake the duties of Data Manager as specified in the Organisational Deed of Licence or MOU;
- Permit the Data Manager to witness the Deed of Confidentiality on behalf of the organisation;
- Within the security measures of the Organisation, permit DSS access to areas within the organisation in which the Datasets are used;
- Notify DSS if the roles of Organisational Delegate or Data Manager pass to a different person;
- Indemnify or reimburse DSS from cost or liability incurred by DSS as a result of actions by users within the organisation regardless of whether those users are Authorised Users or not;
- Acknowledge the Commonwealth as the owners of the intellectual property in the dataset;
- Where the organisation owns the intellectual property in the research material of its staff, permit those staff to provide DSS with research material that uses the datasets; and
- Take responsibility for ensuring that all terms and conditions in the Organisational Deed of Licence or MOU are complied with for as long as the organisation retains the datasets including taking steps to rectify any security breaches by users within the organisation.

In effect, by signing an Organisational Deed of Licence or MOU, the organisation agrees to sponsor individual users within the organisation to be given access to the datasets. Users within

---

1 The organisation will not be responsible for users within the organisation who have access to previous versions of the HILDA, LSAC or LSIC datasets under individual licences but who have not applied for a dataset under the Organisational Deed of Licence.
an organisation that has signed an Organisational Deed of Licence or MOU will only be able to
gain access to the dataset with the sponsorship of the organisation.
Role of the Data Manager

The Data Manager is responsible for ensuring that each user from the organisation uses the dataset responsibly and follows the guidelines provided. The Data Manager is preferably a disinterested party who does not require the datasets for research purposes. If the Data Manager does require the data for research purposes, they must complete the relevant Deed of Confidentiality. The Data Manager has the following responsibilities:

a) Witnessing Deeds of Confidentiality

A Deed of Confidentiality will not be approved by DSS unless it is witnessed by the Organisational Delegate or the Data Manager of the organisation with which the applicant is affiliated.

The application should only be witnessed if the person witnessing on behalf of the organisation can confirm the relationship between the applicant and the organisation and the Data Manager has discussed privacy and security requirements with the applicant.

Data Managers should also check that the deed has been completed correctly.

b) Discussing privacy requirements

Before witnessing a Deed of Confidentiality the Data Manager must discuss the privacy requirements with the applicant to ensure that the applicant understands them fully and is prepared to abide by them. If the Data Manager believes that the applicant will not abide by the privacy requirements, they should not witness the application.

Under the privacy requirements, users must not:

• publish in any form any of the unit record data;
• show or in any way make available the unit record data to anybody other than specific Authorised Users of the dataset (refer to matrix in Fact Sheet 3 Roles and Responsibilities of Authorised Users at e for details about which Authorised Users may share access to the data.);
• make any attempt to identify any of the respondents in the dataset;
• make any attempt to verify identity of respondents if spontaneous recognition (the recognition and potential identification of an individual or household due to the existence of an unusual set of characteristics) occurs;
• inform anybody else about a potential recognition;
• match, merge, link or in any other way join the datasets with any other dataset without prior written approval from DSS (this involves the joining of two or more datasets in order to obtain more information about an individual than is otherwise available in one dataset);

If using the Unconfidentialised dataset:

• the geographic level of detail which may be reported in published research
is limited to State and Territory (e.g. NSW), Major Statistical Region (e.g. Sydney, rest of NSW), Section of State (i.e. major urban, other urban, bounded locality, rural balance and migratory – these are based on population size (only in HILDA)) and Remoteness Area (i.e. major cities, inner regional, outer regional, remote, very remote and migratory – these are based on proximity to a broad range of services). Postcode information available in HILDA and LSAC Unconfidentialised datasets must not be reported on.

c) Security and Administrative Requirements

The Data Manager must make sure that all applicants and users understand and abide by the security and administrative requirements listed in the Organisational Deed of Licence or MOU and the appropriate Deed of Confidentiality. If the Data Manager believes that an applicant will not or cannot abide by the security and administrative requirements, they should not witness that applicant’s Deed of Confidentiality.

d) Coordinating provision of datasets

Data Managers will be sent a copy of the datasets once there has been an approved application for that particular dataset from the organisation. These are the master copies from which the Data Manager may have uploaded to a secure server or make copies of the dataset to provide to Authorised Users within the organisation. Datasets must be kept secure at all times in accordance with the security and administrative requirements in the Deed of Licence.

Datasets may only be provided to Authorised Users. Authorised Users are those who have received written approval from DSS to use a dataset. Authorised Users may only receive the datasets for which they have been given specific permission.

Access to the General Release and Unconfidentialised Datasets may be provided via a password-protected server, or on a CD ROMs/DVDs. The Data Manager must comply with security and administrative requirements as outlined in the Deed of Licence. These details must be recorded in the register kept by the Data Manager. The Data Manager may retain the discs containing the General Release and Unconfidentialised Datasets.

All CD ROMs/DVDs containing copies of the dataset must be handed to the Authorised User in person and signed for by them. CD ROMs/DVDs must only be kept and used only at the organisation’s premises except where prior written approval has been given by DSS.

There must be an effective means of limiting entry during both operational and non-operational hours to rooms or buildings in which the Datasets are used or stored. If possible and where practical, the room must be locked when an Authorised User in not there.

In order to gain access to the datasets on the CD ROM / DVDs sent to the organisation, Data Managers will need a password. This will be sent by the Survey Contract Manager.
Data Managers will need to provide this to users who access the datasets via CD ROM / DVD.

e) Not Providing Data to Unauthorised Persons

The datasets must only be provided to people who have been given written approval by DSS to have access to the datasets. Users must apply for each dataset to which they want access.

Datasets may only be provided through the Data Manager and may not be passed on through other users.

f) Monitoring Users

DSS and its agents conduct random audits of users to ensure that the security arrangements for the datasets are being complied with. If widespread breaches in security are found within an organisation, their Organisational Deed of Licence or MOU may be terminated which will result in loss of access to the datasets to all users in the organisation. It is in the best interest of the organisations to ensure that the security and administrative requirements are adhered to at all times by all users.

The Data Manager will be contacted about any audits to be conducted within an organisation. The record of users kept by the Data Manager for tracking purposes may also be audited.

In undertaking any such audits, DSS or its agent will abide by the security requirements of the organisation and only require access to records or premises relating to the use of the datasets.

g) Providing Access to Organisational Premises

Where DSS requests access to the organisation’s premises or documents relating to the use of the datasets on the organisation’s premises and by the organisation’s Authorised Users, the Data Manager will facilitate and assist DSS staff or their agents with this.

h) Providing Current Information about Users

The Data Manager must inform DSS of any changes to the details about the Authorised Users within the organisation including contact details, completion of research, departure from the organisation and security breaches. Users are required to contact their Data Manager to report such circumstances. The Data Manager will then need to update their records and pass on this information to DSS. In some circumstances, Authorised Users will need written approval from DSS if they wish to use or retain the dataset in changed circumstances, such as for changes in the topic of research. If you require an ‘Organisational User Register’ template, this can be requested from longitudinalsurveys@dss.gov.au. Please note this is the same template as describe at biannual reporting on page 13.
i) Returning Copies of Datasets

If the organisation proposes to cease using the datasets, or if they are requested by DSS to do so, the Data Manager is responsible for deleting copies of the datasets from computer servers and for collecting all copies of the datasets from the users within the organisation and either passing them on to DSS or destroying them. Alternatively, the Data Manager may request written confirmation from individual users that they have destroyed all copies of the datasets in their possession. The Data Manager must then provide written confirmation to DSS that all copies of the dataset given out by them have been accounted for and deleted, destroyed or handed over to DSS.

Authorised Users who wish to retain copies of the datasets will need to contact DSS prior to the organisation fully relinquishing their responsibilities. Arrangements may then be made for those users to sign Individual Deeds of Licence.

j) Providing Research Material to DSS

Researchers using the datasets are required to provide DSS with copies of their research.

Researchers can do this by directly entering the bibliographic details of their research into the FLoSse Research repository at http://flosse.dss.gov.au. The FLoSse Research repository contains details of research based on DSS’s three longitudinal surveys. The research is not made directly available in FLoSse. Instead, FLoSse provides links or directions on how interested researchers may obtain copies of the research.

FLoSse is publicly available but is primarily for use by Commonwealth agencies to source relevant evidence based research for input into policy development.

Generally, the research based on DSS’s longitudinal datasets is expected to be made publicly available and must not be for commercial purposes.

Sensitive research that is conducted for the purposes of internal administration of Australian Government agencies other than for DSS or for confidential business purposes for the Australian Government other than for DSS does not have to be provided to DSS or entered into FLoSse.

k) Maintaining a Register of All Authorised Users

The Data Manager is required to keep a register of all Authorised Users within the organisation. This will include contact details, application details, details of dataset holdings and a description of the research project. For a list of all required fields please refer to Organisational Final Report Pro-forma at page 13.

The Data Manager must provide DSS with an update of all Authorised Users within the organisation confirming their continued affiliation with the organisation, contact details,
the status of dataset holdings, an update of research (i.e. whether finalised or not) and
other information bi annually. An email request for this information will be forwarded to
Data Managers bi annually in September/October of the year Organisation reporting is
due. This update is required before users at the organisation will be able to have
access to new releases of the datasets.

If a user has had a previous release of data from one of the surveys, they agree in
signing the Deed of Confidentiality that they will abide by the terms and conditions in the
Deed of Confidentiality in relation to all releases of the datasets held by them. Signing a
Deed of Confidentiality covers all previously held datasets. The Data Manager must be
aware of all dataset releases held by users and record these and apply the same
security and reporting measures. This information will need to be recorded in the
register. Should the provision of relevant details for the register not be able to be done in
a manner consistent with applicable State/Territory law, access to the datasets will be
withdrawn.

I) Retaining Copies of the Dataset

For some organisations, it may be necessary to retain earlier releases of the HILDA,
LSAC and LSIC data or work containing unit record data once the Authorised User
responsible for them has left the organisation. The user must still fully relinquish their
responsibilities in such an instance by passing the work containing the unit record data to
the Data Manager. The data then becomes the responsibility of the organisation and may
be used by another Authorised User in the organisation. The organisation cannot fully
relinquish their responsibilities for the data while they retain any unit record data.

Additionally, the Data Manager will arrange for the organisation’s payment of the datasets
for each of the surveys with the first application for a dataset from each survey.

Note: For HILDA data - upon payment of your invoice, your dataset and password
access will be sent via Express Post (or Express Courier International for overseas
users).

M) Data Manager Leave

If the Data Manager is on leave, the Organisational Delegate may nominate a substitute
person to fill the role. The Organisational Delegate will need to send an email to
longitudinalsurveys@dss.gov.au stating the name of the person to undertake the role of
Data Manager and the duration of the period that they will be filling the role. The permanent
Data Manager will need to ensure that the person taking on the role during their absence
fully understands the responsibilities of the role. Notification templates from page 13.
Who is Eligible for Access to the Datasets?

Access to the datasets is at the discretion the Department of Social Services (DSS).

Following is a list of the types of users who may be considered for access to HILDA, LSAC and LSIC.

**Users in Australia**

- Academics at an Australian University, Institute of Technology or TAFE;
- Researchers or research assistants, attached to an Australian University, Institute of Technology or TAFE. *Note: In the case of research assistants DSS reserves the right to require a senior research officer working on the same research project to also have access to the same or higher level dataset. This is required in the case of students working as a research assistant. If DSS has any questions about your position, they will contact you directly;*
- Australian Honours*, Masters and PhD students at an Australian University, Institute of Technology or TAFE. *Note: Both the student and their supervisor must apply for access to the dataset independently and must be from the same institution. Supervisors must have independent access to the same or higher level dataset for which the student is applying;*
- Employees of an Australian Commonwealth agency; (including DSS);
- Employees of an Australian State/Territory agency;
- Researchers from community based organisations;
- Researchers within statutory bodies whose primary business is research;
- Individuals within other statutory bodies. Note that this category of applications will be granted access on a case-by-case basis.

* Australian Honours students will only be given access to the data under organisational licensing arrangements.

Other Australian users whose prime business is research may be given access to the datasets if it is to be used for non-profit purposes. Applications for the datasets will be considered on a case-by-case basis.

**Overseas Users**

Overseas users may apply for only the General Release datasets either through organisational or individual licensing arrangements if they fit into one of the following categories.

- Academics at an overseas university.
- PhD students at an overseas university*. *Note that both the student and the supervisor must apply for access to the same dataset independently and both must be located at the same university.*
- Researchers at overseas government agencies who intend to use the data for research purposes.
- Overseas researchers who work at a private institution whose primary business is research and who intend to use the data for research.
purposes.

* Applications from overseas Honours and Masters Students may also be considered for access to the data but only under organisational licensing arrangements.

Other overseas users whose prime business is research may be given access to the datasets if it is to be used for non-profit purposes. Applications for the datasets will be considered on a case-by-case basis.
Organisational Bi Annual Report Pro-forma

Bi annually by the 31 October, the Data Manager is required to provide an all-inclusive update of all Authorised Users of the datasets within their organisation. Organisations will not be given access to further releases of datasets unless this update has been sent to DSS.

The following is a list of fields that must be completed for each person who was an Authorised User at the organisation at any time during the life of the Deed. This data must be provided in an Excel format.

User Details
Title, First Name, Surname, Phone Number, Email, Is the user still at organisation? If not, date they left the organisation Current Department (at a university) or Branch (government department)

Dataset Details
Date that Deed of Confidentiality was signed by DSS, Name of dataset received including release number (e.g. HILDA General Release 11, 9 and 6), Date dataset/s received by user, Format dataset was provided in (secure server, CD Rom, DVD), Serial number of CD Rom/ DVD (where applicable), Have relinquishing procedures been followed?, If yes, date of notification to Data Manager

Research Details
Research topic/s, Name of datasets being used for the research, Estimated date of completion, Status of research (ongoing, complete), Date of completion (if complete), Have the bibliographic details been entered into FLoSse?, In what way have LSIC Data Protocols been followed? (Where applicable).

Details should be provided for each dataset provided and each research topic that uses one or more of the datasets. Details should also be kept of all datasets held by the user originally obtained under individual deeds of licence.

If you have not received a template with your approval of Organisational Deed of Licence this can be requested from longitudinalsurveys@dss.gov.au.
Notification Form for change of Organisational Delegate

I ..................................................(Position)...................... notify DSS of a change to the Organisational Delegate for (Organisation) ........................................ effective from …/…/....

New Delegate details:
Name:..............................
Position:..............................
Phone No:..............................
Email:..............................

Signed ..............................

Date …/…/....
Notification Form for change of Data Manager

I …………………………….. the Organisational Delegate for (Organisation)
………………………… notify DSS of a change to the Data Manager (current
Data Manager)…………………………………… effective from …./…./….

New Data Manager details:
Name:…………………………
Position:…………………………
Phone No:…………………………
Email:…………………………

Signed …………………………
Organisational Delegate

Date …./…./….
Notification Form for a temporary change to the Data Manager

I …………………………….. the Organisational Delegate for (Organisation) ……………………………. notify DSS that the Data Manager (current Data Manager) …………………………………… will be taking leave from …./…./…. to …./…./…. and I have appointed …………………………… phone no. …………………… email:……… as temporary Data Manager for the above period.

Signed ………………………
Organisational Delegate

Date ….../…./….
Notification Form for Relinquishing the Organisational Deed of Licence

I …………………………….. the Organisational Delegate for (Organisation) ……………………… notify DSS that this organisation will relinquish our Organisational Deed of Licence effective from …./…./….

The Data Manager (Name) ………………….. has advised all copies of the datasets have been destroyed, please find attached written confirmation including a full list of authorised users from the Data Manager.

Delegate details:
Position:…………………………
Phone No:…………………………
Email:…………………………

Signed ……………………………
Organisational Delegate

Date …./…./….