EAST HERTS COUNCIL DATA SHARING AGREEMENT

Notes & Guidance

Issue 1.0

INTRODUCTION

These notes form part of the East Herts Council Data Sharing Protocol and provide advice and guidance on how to fill out a Data Sharing Agreement form and set up an agreement under the Protocol.

The agreement form should be filled out by the managers with direct responsibility for delivering and receiving the data to be shared and should be signed off by the managers with overall responsibility for the project or data sharing activity.

Managers should also read and take into account guidance issued by the Information Commissioner under 'Framework code of practice for sharing personal information' http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf

1. AGREEMENT TYPE

This agreement is intended to cover the following types of data sharing:

A. Non Personal Data. Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.

B. De-Personalised Data. Information that relates to individuals, but where it is not possible to identify individuals from the information, whether in isolation or in conjunction with other information that the organisation holds.

C. Personal Data. Information that relates to individuals where the individual can be identified from the data and also where the purpose of the sharing is for research purposes, including statistical or historical purposes.

Only situation (C) falls within the remit of the Data Protection Act 1998 and benefits from a special exemption (Section 33 of the Act) which allows data to be used for research even if it was not collected for this purpose. Personal data held only for research purposes may also be kept indefinitely.

Other data sharing situations (i.e. sharing of personal data for other than research purposes) should also be under C. This includes Statutory obligations to share data, the appropriate statutory authority should be explained in box 2 of the agreement form.

The date the agreement comes into force should be specifically stated. The date the agreement comes to an end can be explicitly stated, or stated in terms of notice; for example, "one months notice".

Where a Type C agreement is being drawn up all parties must be registered with the Information Commissioner and have relevant purposes specified in their scope of registration. Evidence this by writing the organisation's registration number in the appropriate boxes of Section 3.4. If there is any doubt about a partners scope of registration the other party(ies) should satisfy themselves on this point by checking the on-line public register of data controllers. http://forms.informationcommissioner.gov.uk/search.html

2. DATA SHARING PURPOSE STATEMENT

This should be used to detail why the sharing is taking place, what data is to be shared, the nature of the processing and the nature of the research purpose (if appropriate).

If you are creating a Type C agreement you need to be aware that the benefit of the DPA Section 33 exemption for research is not absolute and there are a number of conditions that must be met for it to apply:

- The sharing of data for research must not support measures or decisions that relate to particular individuals, or cause substantial damage or distress to any data subject.

- If the data subjects were not aware that their data was to be used for research at the time it was collected then they should be made aware of the new use to which it is being used, **unless** this is not practical or would require disproportionate effort. Cost, time and age of data are valid considerations when considering practicality and effort.

- Where sensitive personal data is being shared without the data subjects explicit consent this can normally only be done where it "is in the substantial public interest".

Use this section to explain how these conditions will be met, if they apply.

3. DATA OWNERSHIP

This defines who owns the shared data, who is sharing it and who owns any derived or resulting data (if appropriate). There is a presumption that the body providing the data owns it unless stated otherwise.

Enter the names and addresses of the legal entities.

If this is a Type C agreement then all parties handling the data should be entered on the Data Protection Register and their scope of registration should cover the processing of data planned. Record their registration numbers in the appropriate places.

4. CONDITIONS ON USE OF SUPPLIED DATA

Detail here any restrictions on what the receiving party can do with the data or how they must process it. Possible conditions could be:

- Who in the receiving organisation may access the supplied data.
- Who outside the receiving organisation may access the supplied data.
- What acknowledgements of help the receiving organisation must give in their publicity, products or publications.
- What fees are to be paid to the supplying organisation.
- What warranties exist on the supplied data.

Conditions relating to the security or disposal of data should be given in Section 6.

5. CONDITIONS ON USE OF RESULTING DATA

Detail here any restrictions on what the receiving party can do with any resulting or derived data (e.g. analysis or aggregated data sets). Ensure that any restrictions on circulation or fees to be paid are clearly stated. The duration of any restrictions should also be stated.

Possible conditions on the resulting data could include:

- The right to consultation prior to publishing.
- The right to correct errors.
- The right to prevent publication, dissemination or onward transmission of resulting data.
- The right to acknowledgement in publication.
- How any royalties or income from the resulting data are to be divided.
- What metadata is to be produced for the resulting data.

6. MEASURES TO ENSURE SECURITY OF DATA

Specify what security measures are to be taken by the parties with respect to how data should be passed, stored, processed and ultimately destroyed. Ensure that clear responsibility for activities is given so there is no doubt about who does what.

Possible security measures could include:

- Who is allowed to access the data.
- The types of protection to prevent unauthorised access to data; e.g. password protection, encryption of data, physical access to buildings, secure rooms, safes etc.
- The types of protection to prevent accidental loss of data; e.g. back-up and disaster recovery procedures, fire and flood protection to buildings.
- What methods will be used to ensure secure destruction of data; for example, shredding, incineration, secure file deletion and over-write.

Be careful to specify security that is appropriate to the situation.

7. RETENTION PERIOD FOR SUPPLIED DATA

Specify when the supplied data must be returned or destroyed.

Where the receiving party owns resulting data it is assumed that they will have the freedom to retain it as they see fit, unless it is specified here.

8. FORMAT OF SUPPLIED DATA

Detail the physical media in which data will be supplied, how it will be structured and what file formats (if applicable) will be used.

9. OTHER CONDITIONS

This is an optional space to specify any other conditions that don't fit elsewhere. Possible uses include:

- The audit requirements that the parties want to operate
- Provisions for post sharing reviews and lessons learnt

- Requirements to produce metadata for derivative works
- Rules on disclosure under the Freedom of Information Act. Where the recipient of the data is a public body they may be required to disclose the data (unless an appropriate exemption applies). In these circumstances the use of a clause requiring the public body receiving the request to consult with the supplying party before making a decision to disclose is recommended. The following is an example:

```
If the recipient of this data receives any requests for
disclosure they must seek comments from the data provider
before any decision is made on whether to disclose the data
sought.  Comments will be provided within ten days.
```

10. DECLARATION OF AGREEMENT & PARTICIPATION

If necessary alter the wording of the declaration to reflect any specific legal considerations all parties have agreed to.

The responsible officers of the organisations sharing data sign here.

11. RECORD OF DATA SHARING AGREEMENTS

A copy of each signed agreement must be passed to the Information Manager who will maintain a central register of agreements.