

Families, Learning and Progression

Data protection

Guidelines for Family Learning providers collecting progression data for adults

Introduction

This paper aims to clarify issues around data protection and the collection and transfer of data on adults.

For the first year of Family Learning Impact Funding, data on children's progress will not be collected. However, it is expected that such data *will* be collected in subsequent years, and guidance will be issued by the LSC and DCSF.

Information on adults	
Information to be collected	Source of information
Name	Enrolment form
Learner reference	Enrolment form
Further learning, employment, social or personal progression	Learner (through survey or informal contact)
Whether learner feels more able to support child's learning	Learner (through survey or informal contact)

Who will have access to the information?

- The provider of the Family Learning provision that the adult learner (and their children, if appropriate) are attending.
- Learning and Skills Council (LSC).

How will the information be used?

The information will be used to:

- Generate anonymised statistical information showing the progression of Family Learning learners.
- Produce individual case study examples to illustrate the progress and progression that can result from Family Learning. These examples will be anonymised, and unidentifiable.

What are the data protection implications?

The guidance given below assumes that all the organisations involved in the collection and transfer of information are registered on the Data Protection Register, and that their registration covers the transfer of data.

Collecting and processing the information on adults is fairly straightforward from a data protection point of view, as long as the learners are informed of the following:

- what information is being collected about them and how it is to be used;
- that you're not collecting more information than is needed for the exercise, and not using it for purposes other than those you've said;
- that you're keeping the data safe and making sure that it's accurate;
- and that you let the learners access the data you're holding about them on request

(See Appendix: *Data Protection principles*.¹)

APPENDIX: Data Protection principles

The eight principles of the Data Protection Act 1998 should be adhered to.² They are:

1. Personal data shall be processed fairly and, in particular, shall not be processed unless it meets **one** of several conditions, the most relevant of which are detailed below:
 - a. The data subject³ has given his consent to the processing;
 - b. The processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract, or
 - c. The processing is necessary for the purposes of legitimate interests⁴ pursued by the data controller⁵ or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

Any of the above conditions could be used for the collection and processing of the learner information, as long as 'sensitive information⁶' is not being collected (which is not required for the purposes of this exercise). Providers collecting information need to be open and transparent with the learners about what information is being collected and for what purposes.

2. data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this act (this includes the rights of data subjects to have access to the data held about them).
7. Appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area.

The information in this guideline is correct at the time of writing (July 2008). However, it is intended to provide general information only and should not be taken as a full statement of the law, or replace legal advice. The information applies to England only.

NIACE cannot be held responsible for any actions based on the information provided here.

Notes

- 1 See Information Commissioner's Office, Data Protection Act 1998: Legal Guidance, downloaded from http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf accessed 12 August 2008.
- 2 This assumes that the organisations involved in the collecting and transferring of information are registered on the Data Protection Register and that their registration covers the transfer of data.
- 3 The data subject is the subject of the information.
- 4 The Information Commissioner takes a wide view of the legitimate interests condition and recommends that two tests be applied to establish whether this condition may be appropriate in any particular case. The first is the establishment of the legitimacy of the interests pursued by the data controller or the third party, and the second is whether the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject whose interests override those of the data controller.
- 5 The data controller is the individual or organisation that is collecting and processing the information.
- 6 Sensitive personal data is defined as information about the racial or ethnic origin of the data subject; his political opinions; his religious beliefs or beliefs of a similar nature; whether he is a member of a trade union; his physical or mental health condition; his sexual life; the commission or alleged commission by him or any offence.