

DATA PROTECTION

This guidance is designed to support agreements on data protection procedures outlined in Section 2 & 3 of this manual, the Partnership and Service Agreements

1. Legal/Statutory Requirements

Under the *Data Protection Act*, DFES guidance suggests it is legitimate for learning providers to ask schools to release data about students' attendance, behaviour, prior attainment and so on, provided schools have informed students (or in some cases the parents/carers) that they will be sharing personal data with the learning provider for the purpose of carrying out educational functions e.g. to ensure the learning provider provides the appropriate level of support for additional needs. It is advisable for the learning provider to see the evidence of written consent schools have obtained from parents/carers/young learners.

Sensitive personal data relating to SEN or behaviour for example may only be disclosed if explicit consent is received from the student and parent/carer. If consent is not received it may be advisable for providers not to accept the young learner. Learning providers may need to remind schools that failure to pass on information could lead to a situation where the safety of the young learner is compromised.

2. Principles of Data Protection

- **FIRST PRINCIPLE**
Data must be processed 'fairly and lawfully.'
- **SECOND PRINCIPLE**
Data can only be processed for 'specified and lawful' processes.
- **THIRD PRINCIPLE**
Data should be adequate, relevant and not excessive to the purpose.
- **FOURTH PRINCIPLE**
Data must be accurate and up to date.
- **FIFTH PRINCIPLE**
Data can only be kept for the duration of the purpose for which it was obtained.
- **SIXTH PRINCIPLE**
Data must be processed in accordance with the rights of data subjects.
- **SEVENTH PRINCIPLE**
Data must be held in a secure manner.
- **EIGHTH PRINCIPLE**

Data cannot be transmitted outside the European Economic Area without the consent of the Data Subject.

3. Definitions

a Personal Data

Means data which relates to a living individual who can be identified:

- from those data
- or from those data and other information in the possession (or likely to come into the possession) of the data controller

This would include information about students, teachers or placement providers.

b Sensitive Personal Data

The act draws a distinction between Personal Data and *Sensitive Personal Data*. Sensitive Personal Data would include “ethnicity, physical or mental health or condition, the commission or alleged commission by the individual of an offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.”

c Data Controller

“A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.”

This is the person responsible for systems for processing data, anyone involved in the organisation or placement of pupils has a responsibility to follow systems as defined by the Data Controller.

d Data Subject

An individual who is the subject of personal data. Students, parents, teachers, placement providers etc.

e Processing

Processing is any operation carried out on the data including obtaining (recording), retrieving, altering, disclosing and erasing including passing on student data to learning providers

f Explicit Consent

For *sensitive personal data* explicit consent must be given by the *data subject*. It is advisable that parental explicit consent be also obtained

This requires active communication with the data subject and must specify the data, and the purposes for which the data is held. This would include specifying what data is passed on to the learning provider.

References

A Handbook for registration can be found at www.dpr.gov.uk

DATA PROTECTION ENSURING GOOD PRACTICE

- **Learning Base**
The educational establishment should seek the explicit consent of the parents to pass on *personal data* and *sensitive personal data* concerning the student to other learning providers.
- **Data Protection Consent Forms**
These should give in writing, reasons why each specific piece of data is required. The information should explain:
 - a The exact nature of the data
 - b The purpose for obtaining the data
 - c What data is to be passed on to the learning provider

(These forms may cover personal data and sensitive personal data)
- **Bulk Student Data (e.g. SIMS or other similar MIS systems)**
Personal data which may have been passed on in bulk for a number of students should be scrutinised, and at an appropriate time, details for students who will not be placed should be deleted.
- **Relevant Data**
Data Controllers will need to be sure that data passed on to other learning providers is relevant and justified.
In particular the need to pass on the home address should be carefully considered in view of child protection considerations.
- **Accident Reporting**
RIDDOR reporting by employers is covered by statute which is one of the exemptions which permit the processing of personal data and sensitive personal data. There is further exemption where the processing of data is required by a Government Department.
- **Student/Teacher Feedback on Learning Providers**
Care will need to be exercised in reporting back on learning placements where the ethnicity etc of the workforce is noted by the student/teacher. In this case explicit consent must be given.
- **Retention of Data**
The Act requires that data be held only as long as is necessary.
Data should be deleted when no longer relevant. Paper records should be shredded.
- **Student Data**
Schools/Governors/LEAs require student data to be held for up to eight years. It may be appropriate for paper evidence to be returned to the Learning Base for storage.

- **Security**
The Act requires that measures be taken to prevent data from being accidentally damaged or lost or processed unlawfully. It is therefore essential that Data Controllers have adequate backup facilities for electronically stored data. Physical security of buildings, rooms, cupboards etc with appropriate control in the use of keys needs to be sound.
- **Data Controllers**
The Data Protection Act 198 requires every data controller processing personal data to notify unless they are exempt. Failure to notify is a criminal offence.

A Handbook for registration can be found at www.dpr.gov.uk

*The approach to data protection should be a **commonsense approach**. The test when considering data protection is to put yourself in the position of the data subject and to consider whether all the processes, procedures, storage facilities, security measure and communication procedures are proper and reasonable.*

N.B. It must be noted that **Child Protection** takes precedence over **Data Protection** when dealing with personal information. All adults involved with students should be made aware of this

Draft Letter to Parent/Carer

Data Protection

Dear Parent/Carer,

Your child will undertake work at a **Work Related Learning Placement** in the near future.

Under the Data Protection Act it is necessary to obtain your permission and the permission of your son/daughter if vital personal information is to be shared with other agencies providing learning experiences for students i.e. other Schools, Colleges, Training Providers and Employers.

This is necessary so that the health and safety of the young learner is protected. It will also ensure that student personal and educational needs are catered for as far as possible.

The principles of Data Protection state that data must be stored safely, can only be used lawfully and can only be kept for the purpose and time span of the project.

Information kept on file would be the same as that which is usually kept by a normal school such as name and address, emergency contact number, essential medical information, information about assessment of educational abilities and behaviour where this might lead to risk of accident to the student or Learning Provider employees.

In exceptional circumstances, where data is of a sensitive nature, but essential to safeguard the interests of the student, your permission to pass on such data will be sought separately.

I would be most grateful if you could fill in the consent form DP 200 - and return it to school via your child.

Yours faithfully

Work Related Curriculum Organiser



Parent/Carer Consent Form

Data Protection

I the Parent/Carer acknowledge that I have read and understood the Data Protection letter.

I hereby give my consent for appropriate and necessary data held at present

by _____ school relating to my son/daughter

(named) _____

To be shared with other learning providers who are providing courses of study and work related learning.

Please print names carefully below in block letters and sign this permission slip.

This is to be returned to the student's school.

Parent/Carer name _____

Signed _____

Student name _____

Signed _____

Date _____

SCHOOL DATA PROTECTION CHECKLIST

The following Data Protection checklist is designed to help Learning Base staff and Learning Providers ensure they are meeting regulations for data protection when students are working off-site.

Name: Role: Date:

		Yes	No	Don't know	Action needed
1	Has a Data Protection Consent Form been signed and returned to school ?				
2	Has a copy of the Data Protection Consent Form been sent to the Learning Provider?				
3	Is the data to be passed to the Learning Provider. a Accurate? b Up-to-date? c Appropriate to the purpose? (see <i>Sensitive Personal Data</i>)				
4	Has bulk data passed via SIMS or other MIS systems been scrutinised by the school's Data Controller before being passed on to the Learning Provider?				
5	Has the Learning Provider: a Been informed that Student Data must be stored safely? b Stated how the data will be safeguarded and who will act as Data Controller? c Been informed that Child Protection takes precedence over Data Protection?				
6	Has the Learning Provider been sent a copy of ' <i>Ensuring Good Practice</i> ' to ensure all parties are working to the same Principles?				

Freedom of Information Act

The Freedom of Information Act has implications for the conduct of collaborative educational provision and comes into force on January 1st 2005.

The Act opens up the access to information held in schools to the scrutiny of the public and aims to promote a culture of openness and accountability amongst public sector bodies. School governing bodies are responsible for ensuring a school complies with the Freedom of Information Act.

The Learning Base (school or college) will be the main centre for records appertaining to students involved in collaborative educational arrangements and will have policies and procedures operating in line with the act. It is reasonable to expect enquiries about information to be channelled through the Learning Base even though a student may be working off site for a substantial part of his/her working week.

Where the Learning Provider is not a public body they will not be directly involved in providing information to the public, but will have a responsibility to provide relevant information to the Learning Base on request. Relevant information means any information which relates to the provision of collaborative education, including the following:

- Health and safety records and risk assessments
- Accident reporting
- Pupil records
- Induction records
- Attendance records
- Student disciplinary records
- Data for audit requirements
- Reports on pupils' progress
- Moderation and quality assurance records
- Documentation on trips and visits
- Insurance documentation
- Equal opportunities policy

NB: Private companies will not be required to provide any information that does not relate to their work as a Learning Provider as part of the response to a Freedom of Information request.

The need to comply with requests for information within 20 days as per 'the Act' might result in difficulties unless:-

1. The information systems at Learning Base and Learning Provider are maintained assiduously.
2. The Learning Provider is made aware of the possibility of information requests being made at any time.
3. The Learning Base informs the Learning Provider at the outset of the 20 day rule.

Useful Websites

www.governorline.info

www.informationcommissioner.gov.uk

www.teachernet.gov.uk

www.governornet.gov.uk

DfES Guidance October 2004

