



## The Eight Data Protection Principles

Anyone processing personal data must comply with the eight **Data Protection Principles** of good practice. These Principles are, in some cases, legally enforceable. Some of them are quite obvious but others are more difficult to understand. What is important is that they all must be satisfied. Complying with one does not exempt you from the other seven. It is vital therefore that staff have a basic understanding of each one. If the Principles are understood, the whole Act will fall into place. The principles are: -

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate and where **necessary**, up to date
- Not kept for longer than is necessary
- Processed in line with the data subject's rights.
- Security.
- Personal information shall not be transferred to countries outside the EEA without adequate protection

### 1. Principle 1: Fairly and lawfully processed

This creates what is called the **Fair Processing Code**. Basically, this means that your school must: -

- Except in limited circumstances, tell everybody, in clear language, that their personal data are being processed (i.e. your school is a "Data Controller");
- Tell them why, again in clear language, your are processing their data (e.g. for the delivery of education or in order to arrange a school trip);
- Tell them about any "non-obvious" purposes for which your school will process their data (e.g. pupil achievement data being submitted to BELB).

Emphasis is placed on "clear language" because hiding your processing in complex terms is not to be regarded as fair. Neither is it regarded as fair to have a fair processing notice in tiny print at the foot of your form.

Lawful means that other relevant laws in connection with the data must be complied with at the same time as the fair processing code. For example, laws such as copyright and the common law of confidentiality.

It is a good idea to make sure that any letters sent from school to parents, that include some form of

reply slip, have a Data Protection statement at the bottom. The statement should include what the information is required for; what you intend to do with it and who you might pass it onto (other than in school). If your slip or form is asking for **sensitive personal data** then do make sure that you get a signature from the parent stating that they understand why personal data is being requested and that they give their consent to it being used by you in the way which you have described.

## **Children aged 12 and over**

The Information Commissioner has stated that children who are old enough to understand what is being asked of them should be given the opportunity to give their own consent with regard to Data Protection issues.

This is because the Data Protection Act applies to people of all ages, not only those 18 and older. Although no guidance has been given as to how to establish that a child understands what is being asked of them, there is a legal case which set a precedent in this respect (*Gillick v. West Norfolk and Wisbech Health Authority*). This established that in general terms, once a child becomes 12 years of age that he or she is likely to be able to understand the implications of what is being asked. This is commonly referred to as the "Gillick Principle".

In light of this, if your school has children of this age, any forms which ask for personal information and which need to have a signature to indicate consent, should inform parents that their child should be given the opportunity to decide for themselves.

If in any doubt as to whether a child does understand what you are asking, it is better to deal with parents, encouraging them to explain.

Together with the fair processing code, the First Principle requires that before any personal information is processed that one of the conditions set out by the Act in Schedule 2 is satisfied first. Where the processing includes any **sensitive personal data**, then a condition from a further schedule (Schedule 3) also has to be satisfied.

### **2. Principle 2: Processed for limited purposes and not in any manner incompatible with those purposes**

This amplifies Principle 1 by adding that your school must have a very specific reason or **purpose** for processing data. Further, the data can only be processed for that purpose and no other and what's more, all other processing must be comparable with the specified purpose. In short, if data are collected for personnel administration then personnel administration is all that you can do with it. You can't, for example, use it to target marketing material from a company offering services, even if they offer to pay you for your time and effort.

There are some very specific rules for data sharing where other organisations ask you for information that you have collected for one purpose and they wish to process for another.

Something to note here though is that where the DE or BELB ask you to provide personal information (such as that about pupils) this is usually in connection with some requirement imposed by law or a Government department.). Requests arising from either of these two examples are legitimate.

### 3. **Principle 3: Adequate, relevant and not excessive**

This means that your school should collect just the right amount of information for the specified purpose - no more and no less.

In order to assess whether you are collecting "excessive" personal data, look at your forms and consider which pieces of information are absolutely critical in order to enable you to do whatever it is you are trying to do. Whatever is left, if this can't be justified as critical, this would probably be considered excessive. You could also place an asterisk next to the fields that are absolutely essential for the intended purpose. This will enable individuals to decide whether or not to complete the fields not marked in this way (although you would usually need to make this clear by saying so on the form).

This is especially important in respect of data collection exercises that have been undertaken repeatedly over a long period of time. Often in such cases, the information originally collected becomes embellished with other information that is collected because it might become useful. This is a classic example of excessive and irrelevant data collection.

### 4. **Principle 4: Accurate and where necessary, up to date**

Personal data **must** be accurate at all times. Steps must be taken at regular intervals (at least annually) to check that your "live" files are accurate and up to date. A good way of doing this is by conducting an information audit, writing to each person and asking them to verify that the data you hold is correct. This can also be achieved by checking the data that you receive against data that you already hold, such as letters from parents.

Another reason for having accurate personal data is to avoid inconvenience or even damage or distress. For example, if you need to contact a parent or carer in an emergency, yet do not have the correct telephone number this could result in distress for both parent and child. The Data Protection Act conveys the right to receive compensation where substantial damage or distress takes place so this could also be costly for school.

It is also important to note that individuals not only have the right of access to personal information that you hold about them, but also the right to have this information corrected if necessary. This is usually done via the Office of the Information Commissioner but can also be enforced through the courts. This latter course of action could potentially attract adverse public attention through the media, which could be bad for the reputation of your school. So, if you're told of a change or become aware of one you must amend all records as soon as possible.

### 5. **Principle 5: Not kept for longer than is necessary**

When any personal data that you hold has served its purpose, it must be disposed of (and disposed of securely). A school record disposal schedule is published on the DE web site. and gives you an indication as to how long certain types of personal data should be retained. In some instances, there are legal obligations in this respect; in others best practice determines this.

Again this has implications in terms of accuracy. The longer you hold "live" files, the longer you will need to ensure that they are accurate. Also, the longer that information is retained after its useful life, the less it becomes relevant and thus inconsistent with the Third Principle. Holding information that no longer has any useful purpose could also be regarded as excessive, which again is inconsistent with the

Third Principle.

It should also be noted that while ever you hold it, individuals have the right of access to information that you have about them (with some exceptions) Even if this is in your archive or basement storage, you must still provide a copy on request. The more information held unnecessarily, the longer it will take to retrieve and prepare for release to the data subject.

#### 6. **Principle 6: Processed in line with the data subject's rights**

There are other important privacy rights, besides those conferred by the Data Protection Act 1998. These include the right to **confidentiality** under common law. Also, those conferred under the **Human Rights Act 1998**, especially Article 8, "the right to private family life and correspondence" These have implications for how personal information can be used by your school. They are particularly important when it comes to disclosing information, or using information for more than one purpose. This is a complex area and advice should be sought...

#### 7. **Principle 7: Security**

This principle is all about having **proper** security for the personal information that you hold but it also has other implications too.

The main emphasis is on surrounding personal data with a suitable degree of security. This does not just mean security on computer systems (such as password protection and the positioning of screens etc.), it also includes organisational security such as locking filing cabinets wherever possible; clearing confidential files from desks (or at least covering them up); making sure that waste personal data is disposed of confidentially by shredding, etc.

One of the most important aspects of security is making sure that you are not disclosing personal data to someone who does not have a right to receive it. This can be done inadvertently simply by allowing a computer screen to be seen through the window of your school office or school reception. Similarly, by placing papers containing personal information in the ordinary waste or recycling bins at school. Disclosures made inadvertently like this are still unlawful and punishable by fines.

A key aspect of the seventh principle, often overlooked, is that it conveys the responsibility of training your staff about security procedures and the requirements of the Data Protection Act. This is in order to ensure that everyone dealing with personal information does so in a manner compliant with the Act and importantly so that they appreciate that they themselves can be individually liable for any breach that they commit.

Finally, this principle imposes another requirement on data controllers, such as schools. This covers situations where contractors or persons other than your staff process personal information on your behalf. In such situations, you must ensure that security checks are undertaken. This is important because any breaches of the Act by such parties would leave your school liable.

#### 8. **Principle 8: Personal information shall not be transferred to countries outside the EEA without adequate protection**

There are equivalent Data Protection rules in all European Union countries. It is perfectly acceptable therefore to transfer personal data to another EU country, as this will be equally protected in them all.

However, the Act refers to the European Economic Area (EEA) - this includes Iceland, Norway and Liechtenstein. It excludes the Isle of Man because it has a Parliament of its own and has not passed

equivalent Data Protection laws. Other countries will be added to the approved list (maintained by and available from the Office of the Information Commissioner) when they have equivalent Data Protection laws. For example, New Zealand, Hong Kong and Switzerland have already been added.

Others, such as the United States, have not (although there are some large corporations in the United States who are part of a "safe harbour" agreement).

At the moment it is best to get the **explicit** consent of the individual first before transferring any personal data outside the EEA.

Please note that publishing any personal information about an individual (which includes photographs) on a school or any other website has the potential of worldwide publication and therefore the data subject should provide explicit consent prior to the publication,

The Data Protection Act contains many detailed clauses that enhance the eight Principles. However, by understanding the generality of the Principles and applying them to working practices staff will be able to comply with the Act.

FOI/LJ BELB 2007