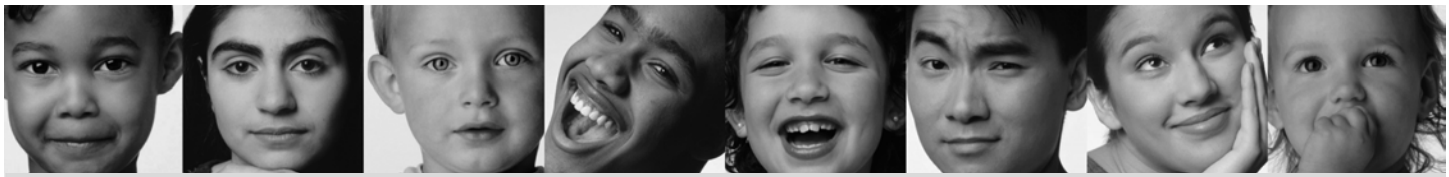
Implementing the Data Protection Act 1998

A Guide for Schools

October 2004



Excellence in Learning

Education Leeds

Table of Contents

Implementing the Data Protection Act 1998 – A Guide for Schools

Executive Summary

The Data Protection Act has many implications for businesses, public authorities and individuals alike. Schools are no exception to this and are subject to all the provisions of the Act, some of which are difficult to interpret. This guide sets out the key areas where Data Protection comes into direct contact with school business and attempts to offer easy to understand solutions with a good range of alternative sources of help if required.

To non-experts in this field, it must seem like a simple step from notification to actual processing of personal information; but in between what are apparently simple steps there are large potential pitfalls in the shape of criminal offences and fines. The guide sets out the key considerations required in order to justify why schools process (or use) personal information and highlights those most relevant.

At the heart of the Act are eight data protection principles which govern the way personal information can be used. It is only right that significant attention is paid to these in the guide. This ranges from specific sections about each individual principle to practical examples of their application through some detailed scenarios.

Of particular note is the advice given in respect of sensitive personal information. Schools hold large amounts of this, most notably in order for reporting to the DfES. This type of information demands special care and attention as it is the kind of information which most individuals are likely to regard as very personal indeed. This is especially true when considering disclosures. Consider how you yourself would feel if information pertaining to your sexuality or state of health was shared with others by someone with whom you have entrusted it. Schools are the guardians of so much information of this nature yet are also the focus of many demands for access to this. Good practice guidance is set out here for schools to consider and with the help of this, an enhanced reputation as a safe repository for personal information will follow.

The guide explodes the common myth that Data Protection is only concerned with information stored on computers. Whilst once true, the new Act concerns itself with all media and this is reflected in this guide where you will find reference to paper, audio, video, photographs, camcorder footage, internet sites and of course computerised records too.

No discussion of the Data Protection Act would be complete without reference to the rights which it confers to individuals. These rights are explained in a way which demonstrates to schools how each one could impact on their daily business and advice is provided on how to avoid pitfalls whilst still recognising the obligations they confer.

Such a guide would also be incomplete without reference to fines and enforcement, especially as individuals can find themselves in breach of the Act and personally liable for the fines and damages which might result. Providing staff with a basic awareness of the requirements of the Act and making a guide such as this available will help to avoid such unfortunate circumstances ever arising. The penalties available to the Courts for offences committed due to breaches of the Data Protection Act are substantial. In some instances both fines and damages can be unlimited in size if the breach is particularly severe. There are already examples of the Act being used to prosecute organisations and individuals and at least one case is used to illustrate this point.

To make this guide as complete as possible, several templates have been provided which schools may adopt, should they choose to. This is in acknowledgement of the increasing demands placed on them and recognition of the fact that it is unreasonable to expect schools to have their own in-house expert on such legislation. An extensive glossary of terms is also included to explain what exactly some of the more uncommon vocabulary used means.

A reference guide about retention rates is included as an appendix to help schools to identify which records can be retained and which can be securely disposed of. There have been many requests for something of this nature over the years. As we get requests for information on this and a range of subjects, we have attempted to cover most of these in our frequently asked questions section which attempts to focus into specific areas of Education Leeds.

As will be obvious, laws change all the time as a result of case-law, public opinion and Government initiative. We have recognised this fact and have thus created a guide which can be added to and corrected as and when the law requires. This will mean that schools only need insert occasional new pages and sections when new guidance is available, rather than having a complete new version of this handbook.

We hope that you will find this guidance useful and would encourage you to provide us with your comments.

"Information Padlock" is a symbol used to alert people to the fact that their information is being collected, and to direct them to sources which will clearly explain how their information is to be used.

Introduction

Schools need to be fully committed to the Principles of Data Protection and should strive to ensure that the highest standards of personal data management are adhered to. This law affects all schools and in some respects there are even specific clauses for education services and schools themselves.

Data Protection applies to all staff – from the Head Teacher to the most junior staff. ***It is everybody's responsibility.***

Data Protection is both simple *and* complex at the same time. The basic idea that personal information must be confidential may be obvious. However, the Act itself is complex and many of its concepts are new and difficult to translate into practice at the sharp end of school business. Please read this Guide. Hopefully, most of it will be easy to digest. If however, any points are complicated or unclear, ask the Information Policy Section (0113 2477889, 0113 3950780 or educ.info.policy@educationleeds.co.uk) for extra help.

The Data Protection Act 1998 is still quite new in terms of the introduction of its powers, many of which didn't come into force until October 2001. It is a very complex piece of legislation that has yet to be extensively tested in Court although there is some case law. This Guide is not a definitive statement of law. It is a Guide for current best practice and this will inevitably evolve as time goes by. The important thing to remember as you read this document is that if you are in any doubt, please don't hesitate to ask the Information Policy Section for help.

This guide has been written to give every member of staff at whatever level of responsibility a basic understanding in Data Protection. It will attempt to explain their responsibilities and give examples of how data protection will affect the way they work. We have tried to cover as many school based scenarios as possible using examples where we have already had direct experience in providing advice to Leeds schools. We have also worked closely with Education Leeds services to identify key interactions between themselves and schools in order to provide advice and guidance in this respect. We have also drawn on national guidance in order to provide a guide that is comprehensive and a single source of reference for all school based staff. You can also access this on the InfoBase Schools intranet site where we will provide access to an electronic version of the guide which can be easily navigated.

We intend to issue you with updates to this guide whenever the law changes. Also, over the course of the next year we will be writing further guidance for schools on other Acts of which you need to be aware. These include the Freedom of Information Act 2000, the Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998. All of these will be designed so that they may be inserted in space already provided in your binder.

Finally, in this guide you will see words and phrases marked in bold like ***this***. Where this is the case, you can look up each of these words or phrases in the glossary at the end of this guide. There are other pieces of text highlighted like ***this***. These are important points, which we have chosen to stress because of their importance. Others are highlighted like **this**. Such highlights have been included to let you know that there is a specific section of this guide dealing with the subject in question, which can be found by referring to the index.

Why Data Protection?

The growth in the collection and analysis of personal data has many benefits both for society as a whole, like helping to fight crime, and for the individual, like better education services. However, whenever personal data are collected and used, people's lives can be adversely affected if something goes wrong. For example, if details are not entered correctly people can be unjustly refused benefits like free school meals, housing, or even a job. If data are not kept securely, people's privacy can be affected, in fact ***identity theft*** is the fastest growing crime in the United Kingdom. It is vital therefore, that those organisations, like schools, which collect and use personal data maintain the confidence of those who are asked to provide it by complying with the requirements of the Data Protection Act (DPA).

The Act gives legally enforceable rights to individuals (called ***data subjects*** in the Act) and places obligations on those who control the data (called ***data controllers*** in the Act, e.g. your school) about the way that personal data can be processed.

Data can, of course, be held on ***computer*** and in ***manual*** files (i.e. on paper files or record cards). Data Protection makes no distinction about where or how personal data are held. If they are about a living individual and are stored with the intention of processing in any conceivable way, Data Protection rules apply.

For the individual, the key to Data Protection is ***personal privacy*** and ***confidentiality***.

The first data protection principle requires that personal data must be processed fairly and lawfully. So, wherever your school wishes to use personal data, you must show that you have considered whether this would be fair to data subjects, taking everything relevant into account. This is a serious and complex duty that can only be met by all staff adopting the highest standards of data management together with a basic understanding of the Act and its consequences.

Your School

Your school is a legal entity in its own right and it collects and makes decisions about the use of ***Personal Data***. This means that the Data Protection Act regards your school as a ***Data Controller***.

Being classed as a Data Controller means that your school has personal data that is owned and controlled by you; for example, details of your staff, pupils and parents or carers. You must therefore comply with the data protection principles and ***notify*** your processing to the Information Commissioner.

Notification

In order to provide an explanation of why your school has to notify, it is essential to explain some legislative background.

The Data Protection Act 1984 (the old Act) required individuals or organisations that processed data on computer to register with the Data Protection Registrar, with few exceptions. A 'data user' was a legal 'person' - an individual, a company or a corporate body. As schools were not regarded as legal 'persons', they could not be data users.

In addition to this, education legislation divided the legal duties connected with the operation of schools between the governing body, the head teacher, and in the case of LEA maintained schools, the local authority. As a result, schools which used a computer to discharge any of the legal responsibilities of the head teacher and governing body had to be registered appropriately - once for the head teacher and once for the governing body, even though the head teacher and governing body may not themselves have been involved in the actual processing of the data.

The Government made clear its intention to end the existing requirement for two registrations when the Data Protection Bill was passing through Parliament. Under the Data Protection Act 1998 (the Act), the existing registration scheme was replaced by a similar scheme of '***notification***'. The Data Protection (Notification and Notification Fees) Regulations 1999 contain details of the notification scheme. Paragraph 6 of the Notification Regulations states that one notification may be made covering the governing body and head teacher in the name of the school.

If your school's governing body and head teacher have each registered under the 1984 Act, it is likely that the two register entries will expire at different times. Where this is the case, your school will now be required to notify at the time the first of these register entries expire. The second register entry will need to be removed at the time of notification. The fee for notification is £35 for one year. Your governing body or head teacher will be sent the appropriate forms prior to the expiry of the first of their register entries.

An application for notification can be made either via the Commissioner's website (www.dataprotection.gov.uk), using the purposes set out in the "Leeds LEA School Notification Template" (available on InfoBase Schools and as an appendices to this guide) or by telephoning the Information Policy Section (Education Leeds) on 0113 2477889 or 0113 3950780.

The Leeds LEA School notification template (**Appendix 8**) has been designed to cover the specific activities of your school and will ensure compliance with this requirement of the Act. Once the forms are complete they will need to be signed by the Head teacher and returned to the Commissioner's Office with the £35 fee. Alternatively, you may wish to send these papers to Financial Services with a request that they raise a cheque from your school budget share and send this, together with your notification papers, to the Commissioner's Office direct.

Finally, please note that the official address of the Information Commissioner is as follows:

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Bogus Approaches

Any approach to you in respect of notification showing a different address may be bogus. We are aware that certain organisations are approaching schools with a letter threatening legal action and requesting a fee of £95 + VAT. If you receive such an approach then please contact the Information Policy Section immediately for advice.

The 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

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 Education Leeds).

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*** (see the section on **Sensitive Personal Data** on page 8) 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. A sample of a declaration covering these implications can be found later in this guidance at **Appendix 12**.

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*** (see the section on **Sensitive Personal Data** on page 8), then a condition from a further schedule (Schedule 3) also has to be satisfied. For more information about this, **see "A Good Reason for Processing**" on page 7.

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. These are mentioned in the section on "**Data sharing**" in this guide. See also the section entitled "**A Good Reason for Processing**".

Something to note here though is that where the DfES or Education Leeds 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 (such as the DfES itself). Requests arising from either of these two examples are legitimate although it is good practice to establish which particular statute or directive applies.

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.

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 writing to each person and asking them to verify that the data you hold is correct. This may be automated by sending data checking sheets from your Management Information System (SIMS). This can also be achieved by checking the data that you receive against data that you already hold, such as letters from parents.

This takes on extra significance in schools for several reasons. The first of these is that the information held on your SIMS system, for example, is required as part of the Pupil Level Annual Schools Census (PLASC). This information is passed to the DfES via Education Leeds once every year. It is used for a number of purposes including the calculation of your school budget share by applying the agreed formula. It becomes obvious that if your funding is based on inaccurate data then so will the funding be inaccurate. Furthermore, for each subsequent purpose for which your original information is processed, if inaccurate, the results of any subsequent processing will also be inaccurate. In the example of PLASC, this has implications for national policy making because the DfES and other central Government departments ultimately use your data for this purpose.

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.

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). The section in this handbook entitled **"Guidance for Retention of Personal Data**" 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 any information that you have about them (with some exceptions, see "**Right of subject access**"). Even if this is in your archive or basement storage, you must still provide a copy on request (with some exceptions). The more information held unnecessarily, the longer it will take to retrieve and prepare for release to the data subject.

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 (see page 14 of this guide). Also, those conferred under the ***Human Rights Act 1998***, especially Article 8, "the right to private family life and correspondence" (see page 13 of this guide). 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 and in these circumstances staff should refer to the guidance notes on "**Data Sharing**" and "**Disclosure of Personal Data**".

There is a section later in this guidance entitled "**Individuals' Rights**" on page 25, which provides more detail.

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.

The section on **Disclosure of Personal Data** should be referred to for more guidance in this respect.

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. An example of a security check questionnaire can be found at **Appendix 7**.

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, (see **Appendix 5** Code of Practice for Use of Images)**.**

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 complying with the Act.

A Good Reason for Processing

Schedule 2 of the Data Protection Act contains conditions, one of which ***must*** be satisfied before processing can commence.

This is about having a good reason for processing personal data and this is one of the most important parts of the Act. In short, if school does not have a good reason to collect and process the personal information in question then a breach of the Act will occur.

Fortunately, there are a number of good reasons contained in Schedule 2 which school should be able to rely on. ***However, these only apply to non-sensitive personal data. For sensitive personal data, a further condition under Schedule 3 must also be satisfied (see page 12 below).***

The Schedule 2 conditions are: -

The data subject has given consent – This is the easiest option. Ideally, fully informed consent should be obtained first. Consent must be fully informed in order for it to be regarded as fair (see **Principle 1: Fairly and lawfully processed**). By fully informed, it is meant that the person being asked to give consent understands what will happen with the information (i.e. what is the intended processing for); why it is required (e.g. because of the requirements of an Act of Parliament and which one); to whom it might be disclosed; the identity of the organisation that will process the information and any other information to ensure fairness. If consent cannot be obtained then one of the other justifications set out below must be satisfied.

Necessary for the performance of a contract – This reason for processing is in respect of contractual clauses and steps that might be necessary for entering into a contract. An obvious case here is the contract of employment with your school or local education authority. Processing in order to enter into a contract could be something like an aptitude test or credit scoring for example. This might also include anything reasonable written into your contract, such as taking a medical at regular intervals to ensure fitness for work for example.

Necessary for the exercise of functions required under a statutory duty - For much work in the public sector, including schools, this reason will often apply. If an Act of Parliament says that we must do something, then there is a statutory duty. This is the case with the statementing of pupils for example and also in the case of provision of information to the DfES under the Pupil Level Annual Schools Census (PLASC). Even though we may have a legal duty to use personal information because of the requirements of an Act of Parliament, we must still tell the person whose information we are using that this is the case.

Necessary in the vital interests of the data subject – This condition must on be relied upon with great caution. It is meant to apply in "life or death" circumstances or where children might be at risk from abuse. For example, where it is necessary to provide sufficient personal information to an ambulance crew following an accident to a child at school who requires hospitalisation as a result. Under such circumstances it is clearly necessary to provide sufficient information in the child's vital interests. However, disclosure of someone's personal details to a company wishing to market a service in which they might be interested is not a valid reason for using this condition, as the disclosure is not in their "vital" interest.

Necessary for the exercise of public functions – This condition includes the administration of justice (i.e., the Courts or the Police), any functions which are required by law (such as the local education authority for example), for the exercise of any functions of the Crown, a Minister of the Crown or a government department (such as the DfES), or the exercise of any functions of a public nature exercised in the public interest (this might include libraries and schools for example). This condition could not be relied upon to cover ancillary processing such as that necessary for the organisation of a school trip for example, as this is not necessary (or vital, in other words) for the exercise of the actual function of a school. Your school can use this condition to justify data collection for the purposes of ensuring that the information you include in your PLASC return is accurate and up to date.

Necessary for the purpose of legitimate business interests – at first glance this seems to be entirely open ended and an easy option to use for any processing which an organisation might choose to undertake. However, the wording associated with this condition makes it clear that any unwarranted processing or any which is incompatible with the rights and freedoms of the data subject cannot rely on this as an excuse to process for just any purpose. In schools, it is likely that this condition can be relied upon to justify processing for such things as staff development, which is clearly necessary for school's legitimate interests (i.e. in order to enhance the skills and abilities of its staff).

It is vitally important to note that all but the first condition in schedule 2 contain the word "necessary". Any processing which is not necessary cannot rely on use of any condition other than consent.

It should also be noted that even when one of the above conditions has been satisfied, in order to satisfy "fair processing" requirements, the data subject must be told who will be processing his or her data, what the intended processing is, what their information will be used for and to whom it might be further disclosed. It may also be necessary (in some cases) to inform the data subject of their rights, such as those available with which to object to direct marketing for example (see section on **Individual's Rights**).

It is also important to note that if you are relying on powers under another Act that these powers must be correctly observed in order for the processing to remain lawful. An example of this is covert surveillance whereby an individual is being covertly monitored (i.e. the person doesn't know that this is taking place) in order to achieve a set purpose such as the prevention or detection of crime. The Regulation of Investigatory Powers Act 2000 makes clear that where such activities are undertaken by public authorities, such as schools, each instance of covert surveillance must be properly authorised using prescribed forms. In the absence of this, the surveillance (which is still a form of processing) will be unlawful and thus in breach of the Data Protection Act.

Sensitive Personal Data

The 1998 Act introduces a new class of data, known as "***sensitive personal data***". This covers the following categories of information:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Health
- Sex life
- Criminal proceedings or convictions

Any personal data in these classes has *extra protection* in law. The most important point is that ***schools must be able to satisfy one condition from Schedule 3 as well as one from Schedule 2 before any processing can take place.***

The first condition in **Schedule 3** creates one of the most important rules in data protection:

"Explicit prior informed consent"

- "**Explicit**" means that the indication of consent is unambiguous and is demonstrated by a signature or some other positive indication
- "**Prior**" means they must have agreed in advance before processing starts
- "**Informed**" means they must understand what they are consenting to
- "**Consent**" means the data subject must have agreed with the processing

The obvious practical difficulty is deciding whether the data subject understands what they are agreeing to. This is very difficult, especially in relation to the Gillick Principle and schools may well have clients for whom informed consent will pose problems. Where this is the case, schools are invited to work together with the Information Policy Section of Education Leeds in order to agree working practices to cope with this requirement.

Schedule 3 of the Data Protection Act provides several conditions other than "prior informed consent" for the processing of sensitive personal data. The main ones on which schools might rely are: -

- Necessary for exercising any legal obligations in connection with employment – in other words it is required by law for personnel and pay matters

- Necessary in the vital interests of the Data Subject or another person – the "life or death" scenario again. Note however the inclusion of "another person". This might cover instances where, for example, a pupil has a contagious disease, which is life threatening and it becomes necessary to warn other pupils of the risk of infection.

- The sensitive personal information has been made public by deliberate steps taken by the data subject. This includes instances where, for example, the child in question has been the subject of a newspaper article including reference to his or her illness.

- Necessary in connection with any legal proceedings, for obtaining legal advice or for the purpose of establishing, exercising or defending legal rights

- Necessary for the administration of justice, (such as court cases and dealings with the Police); necessary for exercising of any statutory duty (e.g. the law says that school must do something such as provide the PLASC return to the DfES); necessary for the exercise of any functions of the Crown, a Minister of the Crown or a government department

- Necessary for medical purposes and undertaken by a health professional or other person who owes a duty of confidence equivalent to that of a health professional (such as a school nurse for example)

- Necessary for maintaining equality or addressing inequality in connection with racial or ethnic origin

Please be aware that many school data files (computerised and paper based) will contain some sensitive personal data and therefore a condition from Schedule 3 (such as those indicated above) must be satisfied as well as a condition from Schedule 2.

Schools may also have to add improved security to some filing systems if they contain large amounts of sensitive personal data. This ***must*** be included in any agreed working practices made in respect of Data Protection.

Disclosure of Personal Data

Under the Data Protection Act 1998 it is an offence to process personal data without the purpose having been notified ("registered" in the terminology of the 1984 Act). Disclosure is itself a process.

Notification includes informing the Information Commissioner of the ***"Recipients"*** of data under each purpose for holding that data, i.e. the persons or organisations to whom data may legally be disclosed. Amendments can be made to notifications/registrations to allow additional disclosures where these are consistent with fair processing, but any amendment must happen before the disclosure takes place.

At the time of collecting personal data from individuals, the information provided to them, must include: -

- the identity of the data controller (i.e. your school name) ***and***
- the purpose(s) for which the data are intended to be processed), ***and***
- the identity of any recipients of the data.

Again if additional disclosures are to be made these would need to be consistent with *fair and lawful processing* and data subjects would have to be given a ***"fair processing notice"*** describing the disclosures to be made. This notice will usually need to be given before the data are first disclosed.

Where personal information is to be disclosed, for example following a ***Subject Access Request*** (see "**Individual's Rights**"), this might entail the disclosure of information about third parties. The third party information may be disclosed only: -

- Where the third party has consented to the disclosure of the information, or
- Where it is reasonable in *all* the circumstances to disclose without the consent of the third party.

To comply with these requirements, new procedures are needed to cover the multitude of circumstances under which a disclosure may take place. This section summarises the overall requirements and provides guidance as to what schools should consider.

- Recording Disclosures

It is now vital that school properly records all disclosures. This is necessary for a number of reasons, including: -

- Awareness as to who has made requests
- Providing an audit trail of events
- For complaint handling
- For onward notification of data errors

This last point is critical. In the unlikely event that an error is found in personal data, school may need to take urgent action to contact everyone to whom it has disclosed the data and to inform them of the correction. A practical approach is needed to ensure that this can be done with the greatest efficiency. **Appendix 1** contains guidelines for schools to follow.

The information stored about each disclosure need not be complex. **Appendix 2** contains a summary of the important things to note about each one.

- Handling Requests for Disclosure

Even if the potential disclosure has been included in the Notification to the Information Commissioner, there is ***no*** right to disclose ***unless*** the First and Second Principles are also complied with.

There are a number of important conditions that apply to disclosures of personal data. These are provided below and to make this clear, the logic is *either* (1+2+3) *or* 4.

1) The nature of the disclosure ***must*** be declared ***in advance*** in school's Notification ***plus***

2) The disclosure ***must*** satisfy the First and Second Data Protection Principles, i.e. it must be done with "***prior informed consent***", or one of the other statutory conditions for fair processing in Schedule 2 (and Schedule 3 in the case of "sensitive" personal data) must be met ***plus***

3) The requirements of the Fair Processing code must be met, i.e. if data subjects were not told when the data was first collected that a particular disclosure was likely to be made, then school must provide a written notice describing the disclosure to be made ***before*** this takes place

   Or

4) There must be a legal duty to disclose the data in question as specified in the section on "**Compulsory Powers**" later in this section.

- Crime and Taxation

There is a general exemption in ***Section 29*** of the Data Protection Act that will allow schools to disclose to the relevant authorities personal data for the purposes of: -

- The prevention and detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of any tax or duty (or similar)

This exemption only applies however, when to withhold the data "would be likely to prejudice those purposes".

This general exemption will apply primarily to the Police and they will be the main agency that will be requesting personal data under S.29. However, it is important to remember that there are a number of other agencies that can also make requests under S.29. Other relevant authorities include the Local Authorities (Council Tax), the Inland Revenue and Customs & Excise, all of whom have tax gathering powers.

The secret security services (MI5, etc.) are generally exempt under "***national security***" considerations. However, such agencies are unlikely to approach schools, although it is possible.

It is important to understand that the provisions of S.29 do not compel schools to disclose personal data unless withholding the data "would be likely to prejudice those purposes" as stated earlier.

Schools will be subject to specific legislation that applies to their work and staff should be made aware of any special circumstances for disclosure provided in this. Such special circumstances apply in respect of Child Protection whereby information can be disclosed to certain authorities including Social Services and representatives of the Area Child Protection Committee.

- Requests for Personal Data under Crime or Taxation Powers

Schools will need to make a judgment as to whether or not there is likely to be any prejudice to the prevention/detection of crime etc. in relation to the circumstances of each individual case.

This may be difficult in practice. It will be especially difficult for individual members of staff to make appropriate judgements when agencies such as the Police approach them for personal information. Any such requests should therefore be directed to the Information Policy Section of Education Leeds if in any doubt.

Where the Police, Inland Revenue and Customs & Excise are involved, all of these organisations have their own pro-forma, which they should use when requesting personal information. Each form should state precisely which statutory powers apply and in general terms, why they are seeking information.

These requests must only be about specific investigations. They cannot be used for "fishing" exercises and any attempt of this nature should be rejected.

An example of the pro-forma used by West Yorkshire Police (form DP7) can be found at **Appendix 3.**

Copies of pro-forma used by other agencies will be circulated to schools as and when they become available.

- Current Work Practices

A major issue for many schools may be unofficial arrangements that have been developed over the years with other agencies to swap data about individuals. It is difficult to offer examples of this but schools will be generally aware of these practices. They are short cuts and they abbreviate tortuous processes. ***They may also circumvent legal processes***.

The curtailing of unofficial data sharing practices may be resisted as they could be seen as interfering with workflow and may counter established relationships between professionals. There is a real danger however, that individual staff will circumvent the Data Protection Act and even the Human Rights Act at the risk of action by the Information Commissioner or aggrieved individual members of the public.

Perhaps it is pertinent to point out that it is an offence for any person, without the consent of the data controller, (i.e. your school), to knowingly or recklessly: -

"Obtain or disclose personal data or the information contained in personal data, or procure the disclosure to another person of the information contained in personal data" (Section 55).

To disclose data to a third party without justification is an offence for which the maximum penalty is £5,000 in a Magistrates' Court or an unlimited fine in Crown Court. Compensation for damage or distress caused by unlawful obtaining or disclosure is unlimited. If your school discloses information in breach of the Human Rights Act or the Common Law of Confidentiality this may also lead to a claim for damages. See "**Enforcement**" on page 39 of this guide.

- Implications of the Human Rights Act 1998

If your school discloses information which relates to a person's private or family life, or home, or the content of their correspondence, this could amount to *a breach of the right to respect for private and family life, home and correspondence* under *Article 8* of the *Human Rights Act 1998*.

There are only limited grounds, specified in *Article 8.2*, upon which schools (as public authorities) are permitted to interfere with individual's rights. These grounds are: -

- National security
- Public safety
- The economic well being of the country or the Local Council's area
- The prevention of disorder or crime
- The protection of health or morals
- The protection of the rights and freedoms of others

In addition to identifying a specified ground for interfering, schools must also have the legal powers to disclose the information and must try to strike a *fair balance* between that ground and the individual's rights.

If schools receive a request to disclose information, which constitutes personal data under the Data Protection Act, Article 8 of the Human Rights Act will almost certainly cover this and the requirements of this will also need to be considered.

In practical terms, if schools are asked to disclose information, for example in respect of crime prevention purposes, this still cannot be released "automatically" even if they are provided with the appropriate form. Individual's rights must be considered and balanced against what the Police (for example) have told school about the criminal investigation. Again, this will be difficult in practice and it is recommended that such matters be referred to the Information Policy Section of Education Leeds.

- Confidentiality

In addition to the laws already discussed above, the "*common law*" duty of *confidentiality* must also be considered. This duty is not contained in any Act of Parliament but binds schools legally in the same way as the Data Protection and Human Rights Acts.

If information has the necessary quality of confidentiality about it (for example, it's to do with someone's pay or their health) or was communicated or became known to school in

circumstances entailing an obligation of confidence (for example, it was contained in a letter headed “confidential”) and that information is then disclosed, there could be a breach of the common law duty of confidentiality. School may choose to say explicitly on some forms that information will be treated as confidential, or individuals may provide school with information expressly on a confidential basis. In many other cases forms and correspondence will be silent on this. As a general "rule of thumb" it should be assumed that where school holds information about an individual which is private in nature, then that information is likely to be subject to an obligation of confidentiality.

However, this obligation may be outweighed by matters in the public interest, in which case disclosure would be allowed, for example, the prevention of crime or in the interest of public health and safety. It is important to note that disclosure can only be justified to the extent necessary to enable school to perform its function. This is a somewhat stricter test than the data protection and human rights rules.

Again, in each case a balance has to be struck between the obligation of confidentiality and the competing public interest. As is the case with the Human Rights Act, schools need to ensure that confidentiality is dealt with at the right level and is properly recorded.

- Compulsory Powers

It must be remembered that some agencies (e.g. the Police and the Inland Revenue) have legal powers to require schools to disclose information in certain circumstances. Where agencies claim they are relying on these powers they should be asked to specify them. Disclosure can also be required under a Court Order that sets out the data to be disclosed and to whom, usually within an enforceable time-scale. All of the above types of disclosures should be recorded in the same way as described in **Appendix 2.**

Where these powers are exercised, the requirements of the Data Protection Act, the Human Rights Act and obligation of confidentiality are over-ruled.

- Data Processors

It is especially important that disclosures to ***data processors*** are carefully considered before they actually occur. A data processor is any person or organisation (other than an employee of school) who processes personal data on behalf of school. For example, if school were to appoint a company to analyse pupil performance (at individual level) then the appointed company would be performing an action on personal information under the instruction of school. Under such circumstances, school must take steps to ensure that the data processor pays due regard to the requirements of the Data Protection Act. This is very important because in the event that the appointed company breaches the Act, school will be liable for any subsequent fines or damages as they remain the data controller.

Schools are strongly recommended to issue the **“Data Security Questionnaire to Data Processor”** at **Appendix 7** whenever the above circumstances apply. The Information Policy Section can also offer assistance in this respect.

- Disclosures for Research Purposes

Schools can be asked to disclose personal information for legitimate research purposes. There are two practical problems: -

- Making sure that it is reasonable to release the data
- Making sure the researcher understands and meets their data protection obligations

This guidance is *not* about research that is directly commissioned by schools. Under such circumstances there will normally be a separate and formal Contract drawn up with the research agency.

There may be numerous approaches to school to release personal data for research projects. These requests can come from: -

- Undergraduates as part of their studies
- Post-graduate researchers (e.g. PhD students)
- Large scale academic studies (e.g. by one of the major hospitals)
- Special interest groups (e.g. charities)

It is up to each school to evaluate the request and to decide whether or not the request is legitimate. This guidance cannot cover all the possible issues involved but a common sense approach is needed and should consider: -

- Is the student following a formal course of study?
- Is the research institute well known?
- Are there any ethical issues surrounding the request?
- Is the research field outside any education policy areas?
- Is the student/institute willing to share the results?
- Will the research be beneficial to pupils?
- How will the data be reported?

The main concern should be that the research is properly formulated and conducted. Plus, in the case of students, a tutor should properly supervise it.

Genuine research is a permitted use of data under the Data Protection Act 1998. In particular, Section 33 of the Act covers this exemption. This Section is complex but the general principles are: -

- Research is about aggregations of data and not processing any individual's data
- The data subjects must not be harmed in any way by the research
- Research data can be kept for ever
- Research data must still be kept secure

An interesting point is that where personal data is to be used for research purposes and *only* research purposes, the prior agreement of the data subject is not required.

School's notification under the 1998 Act incorporates research activities as a purpose for which personal data may be disclosed.

It may be good practice to make some attempt to inform the subject group that the research is taking place. After all, they may question the validity of any approach by a researcher and ask if it has school's approval. This is a difficult area and precise rules cannot be quantified easily. However, schools should carefully consider this issue and take any appropriate steps they consider necessary to inform the target group. These steps might include: -

- Posters displayed prominently in school
- Leaflets
- Letters to pupils, parents and staff

This is not to say that the subject group must always be informed. In many cases, publicity may be irrelevant because the research may be too remote from school business. The subject group may also be very large making it difficult to notify everyone. The researcher could be asked to contribute to this process, e.g. provide posters, as this may help to increase the take up of the research.

As you have read already in this section about disclosures, the Data Protection Act requires school to be careful how it discloses personal data. While research is a permitted activity, there are dangers that school may incur a liability to an individual if the researcher does not handle the personal data correctly and infringes the Act. In light of this, a draft agreement has been created to manage the release of research data (**Appendix 15**). Its advantages are: -

- It clearly defines the data set to be released
- It states the important parts of the Data Protection Act that apply
- It clarifies the responsibilities of the researcher

This agreement is not intended to admonish school of any responsibility but rather to create a working framework under which both parties can comply with the law.

It is recommended that schools use this Agreement for all research projects not commissioned by them.

- Recommendations to Schools Regarding Disclosures

There are clearly serious obligations imposed on schools in connection with any disclosure of personal, private or confidential information. Schools are recommended to take the following steps to ensure that they comply with their legal obligations: -

- Note *all* disclosures as per **Appendix 2**
- Allocate the task of recording them to an individual or team
- Understand the need to maintain an ***audit trail*** of disclosures
- Make sure all staff are sufficiently trained to handle disclosures within the law
- Take particular steps to make sure that disclosures to the Police or other security agencies are handled correctly and the necessary written request has been received
- Make sure that other agencies with powers to request data provide the necessary written requests
- Be especially aware of the implications of the Human Rights Act and how this may limit school's ability to disclose personal information
- Be aware of obligations in respect of the common law duty of confidentiality
- Issue a "**Data Security Questionnaire**" whenever school uses another organisation to do something with personal information for which school is the data controller
- Issue an "**Agreement to Conduct Research**" to bind any organisation or researcher where this will involve personal information for which school is responsible.

The flow chart at **Appendix 4** gives basic guidance on when and when not to disclose personal data.

This is a very difficult area. The laws are complex and until they are tested in the Courts there is a need to make judgments on the best course of action in any particular case. If in any doubt, the Information Policy Section of Education Leeds should be consulted for guidance on the correct procedure.

Paper (Manual) Files

These were excluded from the Data Protection Act 1984 but are covered by the 1998 version. Manual files containing personal data are now included within Data Protection rules. Therefore, it is important to remember that all of the Data Protection Principles, the rights conferred to individuals and anything else contained in the Act will apply to manual files also.

Schools should ensure that they each have their own procedures to ensure their manual files are up-to-date and as accurate as possible. Although this is an onerous task, staff must make sure that they are fully aware of the requirements of the Fourth Principle (personal data must be accurate and, where necessary, up to date) in respect of manual files.

The Fifth Principle is also important with regard to paper files as this provides that personal data should not be kept for longer than necessary. It is essential therefore to have a good retention policy and that this be rigorously applied, especially for files which are placed into storage and often forgotten. The section in this guide entitled **"Guidance for Retention of Personal Data**" provides useful information about how long different types of information should be kept. Once paper files have reached the end of their useful life they should be confidentially disposed of, for example by shredding. There are a number of local companies providing such services and details of these can be obtained from the Information Policy Section.

Good organisational security should be employed to protect paper files, such as lockable filing cabinets, especially for sensitive personal data. There should also be adequate protection against loss caused by fire and flood, especially if loss of files would cause damage or distress to an individual (for example, the files may be the only record of natural parents of adopted children). This is an important consideration in connection with the Seventh Principle.

Also, it is of great importance to be aware of the fact that any notes or comments you make on a file, be they on a "post-it" note or pencilled onto a copy of a memo, will have to be released should a subject access request be made. It is therefore essential that only appropriate notes and comments are made in this manner as any expression of opinion which could be interpreted as defamatory could lead to legal action. This is also the case for notes and comments made against records on computer systems.

CCTV Systems

Closed circuit television (**CCTV**) is being used more and more, especially in schools, in the fight against crime and disorder. However, it is not only the images of criminals and the unruly that are caught but also those of staff and the public going about their daily business, more often than not totally unaware that they are being filmed. This is in fact a form of processing and our images are certainly personal data (see **Appendix 6**, "**Glossary of Terms**" at the end of this guide). What is more, these images could portray sensitive personal data such as an individual's religion, which may be identifiable from a person's clothing, or a disability may be apparent.

As a result, it is essential that we follow guidelines set out by the Information Commissioner in his "***CCTV Code of Practice***". This sets out standards that should be met when any scheme is put in place. These standards cover the following areas:

- Initial assessment procedures;
- Siting the cameras;
- Quality of images;
- Processing the images;
- Access to and disclosure of images to third parties;
- Access by data subjects;
- Other rights;
- Monitoring compliance with the Commissioner's Code of Practice.

- Initial assessment procedures

The First Data Protection Principle requires that schools must have a legitimate basis for processing personal data, in this case images captured on CCTV. The Act also states that criteria must be met in order to demonstrate that legitimate basis. The surveillance equipment might be intended for one of several purposes such as prevention, investigation and detection of crime; apprehension and prosecution of offenders (including use of the captured images as evidence in criminal proceedings); public and employee safety; monitoring security of premises, car parks and so on. It is important therefore to establish several things in an initial assessment:

- The appropriateness of and reasons for using CCTV or similar surveillance equipment should be assessed and documented in a scheme setting these out
- The purpose of the scheme must then be established (in order to meet the **First** and **Second Data Protection Principles**). The first principle in particular requires that schools must have a legitimate basis for processing as dealt with by **Schedules 2 & 3**
- The identified purpose of the scheme should then be documented
- Once the purpose has been established the, school's ***notification*** entry must be checked to ensure that it covers the purpose(s) put forward
- It should be established and documented who is responsible for ensuring day-to-day compliance with the requirements of the Commissioner's Code of Practice and any which school itself puts in place
- Security and disclosure policies set out by school should be observed

- Siting of Cameras

The Commissioner's Code of Practice emphasises the importance of careful consideration with regard to the location of cameras, in particular, because of the requirements of the First Data Protection Principle (fair processing). These are the standards which the code sets forth:

- The equipment should be sited in such a way that it only monitors those areas which are intended to be covered by the equipment (**First and Third Principles**)
- If domestic areas such as gardens or other areas border the intended spaces to be covered then school must consult with the owners of such spaces if images might be captured from them. In the case of a garden for example, this would be the owner of the property which is overlooked (**First and Third Principles**)
- Staff operating or monitoring the system must be aware of the purpose(s) for which the scheme has been established (**Second and Seventh Principles**)
- Staff should be aware that they are only able to use the equipment for the purposes for which the system has been installed (**First and Second Principles**)
- Any cameras which are adjustable by staff should be restricted so that they may not be manipulated to overlook spaces which are not intended to be covered (**First and Third Principles**)
- If cameras cannot be restricted to prevent spaces not intended to be recorded being covered by the equipment then staff must be made aware of the privacy implications of such spaces being recorded (**First and Third Principles**). For example, individuals sunbathing in their back gardens may have a greater expectation of privacy than individuals mowing the lawn of their front garden.
- Signs should be prominently placed in order that the public are aware that they are entering a zone which is covered by surveillance equipment (**First Principle**)
- Such signs should be clearly visible and legible to members of the public (**First Principle**)
- The size of the signs should reflect the circumstances. For example, a sign on a door may only need to be A4 as this will be obvious to anyone entering the premises. A sign in a car park however, might need to be A3 in size so that it can be seen from further away.
- Signs should contain the following information:
    - The name of the organisation, (i.e. school name), responsible for the scheme
    - The purpose(s) of the scheme
    - Details of who to contact regarding the scheme

  For example, where the sign shows a picture of a camera the following wording might be used: "This scheme is controlled by Sometown Primary School. For further information contact 0113-111-1111".

If there is no picture of a camera on the sign then the following form of words would be more appropriate:

> "Images are being monitored for the purposes of crime prevention and public safety. Sometown Primary School controls this scheme. For further information contact 0113-111-1111".

- In exceptional and limited cases, if it is assessed that the use of signs would not be appropriate, school must ensure that:
  - A specific criminal activity has been identified
  - The need to use surveillance to obtain evidence of that criminal activity has been identified
  - An assessment is made as to whether the use of signs would prejudice success in obtaining evidence
  - An assessment is made as to how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary
  - All of the above is documented
  - A form authorising "***covert surveillance***" under the ***Regulation of Investigatory Powers Act 2000*** is completed and signed by the Head teacher before the surveillance commences and a copy of this form is submitted to the Information Policy Section of Education Leeds

Any information that is obtained where it has been decided not to display a sign can only be used for prevention or detection of criminal activity or the apprehension or prosecution of offenders. It could not be used for instance, to provide evidence for a disciplinary against a member of staff who was filmed breaching school policy.

- Quality of Images

It is important that any images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is so important to establish the purpose at the outset of any scheme. The **Third, Fourth and Fifth Principles** in particular are concerned with the quality of personal data.

The following are the required standards:

- Following installation a check should be made to ensure the equipment performs properly
- If tapes are used, they should be good quality (**Third and Fourth Principles**)
- The medium on which the images are captured should be cleaned so that images are not recorded on top of images recorded previously (**Third and Fourth Principles**)
- The medium on which the images are recorded should not be used when it has become apparent that the quality of images has deteriorated
- If the system records features such as the location of camera and/or date and time, these should be accurate (**Third and Fourth Principles**). A documented system should

also be available for ensuring accuracy

- Cameras should be situated so that they capture images relevant to the purpose of the scheme (**Third Principle**). For example, if the purpose of the scheme is the apprehension and prosecution of offenders and the prevention and detection of crime, cameras should be sited so that images enabling identification of perpetrators are captured
- If facial recognition systems are used, then both sets of images should be clear enough to ensure an accurate match (**Third and Fourth Principles**). Procedures allowing a human operator to verify the match should also be available (**First, Sixth and Seventh Principles**)
- Any determination made by the human operator should be made whether or not there is a match
- Consideration must be given to the physical conditions in which cameras are located (**Third and Fourth Principles**). An example of this is that infra red equipment may be required in poorly lit areas
- An assessment must be made to establish whether constant real time recording is necessary or whether the activities about which they are concerned only occur at specific times (**First and Third Principles**). For example, it may be that a criminal activity only takes place at night in which case it should only be necessary to constantly record images during night time hours
- Cameras must be properly maintained and serviced to ensure that clear images are captured (**Third and Fourth Principles**)
- Cameras should be protected from vandalism in order to ensure they remain operational (**Seventh Principle**)
- A maintenance log should be kept
- If a camera is damaged there should be clearly defined responsibilities for ensuring that it is repaired promptly, within the specified time and done to high quality standards

- Processing the images

Images that are not required for the purpose for which the equipment is intended should not be retained for longer than is necessary. While images are retained it is essential that their integrity be maintained to ensure their value as evidence and to protect the rights of the people whose images might have been recorded. It is therefore important that access to and security of the images is controlled in compliance with the Data Protection Act 1998 and in particular the **Seventh Principle**.

Required standards are:

- Images should not be retained for longer than is necessary (**Fifth Principle**). For example, recording of premises may not need to be retained for longer than 31 days unless they are required for evidential purposes in legal proceedings
- Once the retention period has expired images should be removed or erased securely (**Fifth and Seventh Principle**)

- If images are retained for evidential purposes they should be retained in a secure place to which access is controlled (**Fifth and Seventh Principles**)
- On removing the medium on which the images are recorded for use in legal or disciplinary proceedings, the following should be documented: -
    - The date on which the images were removed from the system for use in the proceedings
    - The reason why they were removed
    - Any crime incident number to which the images are relevant
    - The location at which the images will be held, e.g. police station address
    - The name and signature of the Police Officer collecting the images
- Monitors displaying images from areas in which individuals would have an ***expectation of privacy*** (such as changing rooms) should not be viewed by anyone other than authorised employees of school
- Access to the recorded images by third parties or by any person that has submitted a subject access request will be determined by the responsible person in school for the operation of the system in accordance with established procedures on disclosure (**Sixth and Seventh Principles**)
- Viewing of the images should take place in a restricted area to which unauthorised employees or other persons have no access at the time of the viewing (**Seventh Principle**)
- Removal of the medium on which the images are recorded, for viewing purposes, will be documented as follows:
    - The date and time of removal
    - The name of the person removing the images
    - The name of the person(s) viewing the images including the organisation for whom any third party works or represents
    - The reason that viewing was necessary
    - The outcome, if any, of the viewing
    - The date and time the images were returned to the system or secure place if retained for evidential purposes
- All operators and employees with access to images should be aware of the procedures which need to be followed when accessing the recorded images (**Seventh Principle**)
- All staff responsible for operating the system should be trained in their responsibilities under the Code of Practice and in particular, should be aware of the procedure for access to recorded images, school's disclosure policy and the rights of individuals in relation to their recorded images (details of which are listed below).

- Access to and disclosure of images to third parties

It is vitally important that access to and disclosure of images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled. This is essential to ensure that the rights of individuals are preserved and also to ensure that the chain of evidence remains intact should footage be required for evidential purposes. School must also ensure that the reason(s) for which images may be disclosed are compatible with the reasons or purposes for which they were originally obtained.

It is important that all staff whose work involves some usage of CCTV are made aware of the restrictions set out by the Commissioner's code of practice.

The following are the required standards:

- Access to images must be restricted to those employees that need to have access to the equipment in order to use it for its specified purpose(s) (**Seventh Principle**)
- All access to the medium on which the images are recorded should be documented (**Seventh Principle**). See the documenting procedures set out below
- Disclosure of images to third parties should be limited and made only under prescribed circumstances (**second and Seventh Principles**). For example, if the purpose of the system is the prevention and detection of crime, then disclosure should be limited to the following third parties: -
    - Law enforcement agencies where the recorded images would assist in a specific criminal enquiry
    - Prosecution agencies
    - Relevant legal representatives
    - The media, where the public's assistance is considered necessary to assist in the identification of a witness or perpetrator in relation to a criminal incident. ***However, the wishes of the victim must be taken into account first.***
    - People whose images have been recorded and retained, (unless disclosure to them would prejudice enquiries or criminal proceedings).
- All requests for access or for a disclosure should be notified to the responsible officer in school who will then record details including, if applicable, why a disclosure has been denied (**Seventh Principle**)
- If access to or disclosure of images are allowed then the following must be documented: -
    - The date and time at which access was allowed or the date on which disclosure was made
    - The identification of any third party who was allowed access or to whom disclosure was made
    - The reason for allowing access or disclosure

- The extent of the information to which access was allowed or which was disclosed

- Recorded images should not be made more widely available. For example they should not be routinely made available to the media or placed on the Internet (**Second, Seventh and Eighth Data Protection Principles**).

- If it is intended that images will be made more widely available, that decision should be made after consulting with the responsible officer in school. The reason for that decision should be documented (**Seventh Data Protection Principle**).

- If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable (**First, Second and Seventh Data Protection Principles**).

- If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out.

- If an editing company is hired, then the responsible officer in school will need to ensure that:

    - There is a contractual relationship between school and the editing company.
    - That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.
    - The responsible officer in school has checked to ensure that those guarantees are met
    - The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of school
    - The written contract makes the security guarantees provided by the editing company explicit. (**Seventh Data Protection Principle**)

- If the media organisation receiving the images undertakes to carry out the editing, then the above will still apply (**Seventh Data Protection Principle**)

- Access by data subjects

Everyone has a right of access to any information held about them in school. This is provided by section 7 of the 1998 Act and includes access to their images captured by CCTV or similar equipment. Subject access is discussed in more detail in the section on **Individual's Rights** later in this guide.

Any such request must be directed immediately to the person responsible in school for compliance with data protection or to the Information Policy Section of Education Leeds at the address shown at the end of this guide.

- Other rights

A detailed explanation of the other rights under Sections 10, 12 and 13 of the Act are also provided in the section on **Individual's Rights** later in this guide.

The standards required in order to satisfy these other rights are as follows:

- All staff involved in the operation of the equipment must be able to recognise a request from an individual to:
    - Prevent processing likely to cause substantial and unwarranted damage to that individual
    - Prevent automated decision taking in relation to that individual
- All staff must be aware of the identity of the designated member of staff responsible for responding to such requests
- The responsible officer must provide a written response to the individual within 21 days of receiving the request setting out the decision
- If the responsible officer decides that the request will not be complied with, the reasons must be set out in a response to the individual and a copy of the request and response be kept

- Monitoring compliance with this code of practice

These are the main standards which school are recommended to adopt to ensure that this code of practice is complied with:

- The contact point indicated on any sign should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.
- Enquirers should be provided on request with one or more of the following:
    - The name and work address of the responsible officer in the event that they decide to make a subject access request
    - A copy of this code of practice
- Complaints should be carefully recorded and reported to the responsible officer in order that an assessment can be made. This will also enable the monitoring of public reaction to the scheme and whether it is meeting its intended purpose.

Rights

Apart from the legal obligations under the Data Protection Act that schools are required to discharge, there are a number of ***rights*** that the data subject has of which school staff must also be aware. These rights must not be infringed in any way as the Information Commissioner can enforce them, as can the Courts. The rights in question are as follows: -

- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for direct marketing
- Rights about wholly automated decision making
- Right to seek compensation if distress has been caused
- Right to rectify, block, erase or destroy inaccurate or unjustified personal data
- Right to ask the Information Commissioner for a ruling about whether the Act has been contravened by school

Right of subject access (Section 7)

The right most often exercised is the ***right of access to personal data held about ones-self*** – also known as **"*subject access***". Anybody can ask to see information that school is holding about him or her – this is what "subject access" means. If somebody simply comes to school reception and asks to check an item of information, e.g. their registration details with school, then they should be shown this information providing that they can prove their identity. Acceptable proof includes production of a passport, driving licence or birth certificate. However, in the absence of any other form of proof, comparison of the person's signature with one already held on file is acceptable. A data subject can however be much more formal and ask for written copies of all the information that school holds about them. This is a more complex matter with very specific legal rules. If a formal request is made, it must be dealt with in a set timescale so it is important that is brought to the attention of the responsible officer in school, without delay. Alternatively, it can be forwarded to the Information Policy Section of Education Leeds who can deal with this matter on your behalf although it is essential that this be done quickly for reasons, which will become apparent.

Where education is concerned, there is what is known as a "***statutory instrument***" in force, which changes the rules for dealing with subject access requests, which involve an "***educational record***". An educational record is any record held by a school in connection with a child's education and covers correspondence with the LEA and any support services such as those provided by Education Leeds. "**Statutory Instrument 2000, No.297, The Education (Pupil Information) (England) Regulations**" provides, amongst other things, that where such a request is made, there are ***15 school days*** in which to respond (as opposed to 40 consecutive days for all other requests such as those submitted by teachers, for example). A separate order also provides that schools may charge up to £50 (dependant on the number of pages to be disclosed). **Note**: the maximum charge for access to personal records other than educational is £10. For information, Education Leeds has a no-charge policy in respect of such requests.

A sample form has been provided at **Appendix 13** for use when approached by individuals for access to their records held by school. Please note however, that individuals do not have to use this and may insist instead on sending a letter of request to school.

Right to prevent processing likely to cause damage or distress (Section 10)

The second right is concerned with ***processing that causes damage or distress***. This does not include damage or distress that might be caused to a legal entity such as a school; it is only concerned with individuals. This usually arises where a mistake has been made and the personal data being processed is incorrect, for instance, the registering of an address on credit reference lists for non-payment of debt where the debtor no longer lives there. Or for example, where a child is refused a free school meal because incorrect information has been used to determine whether or not he or she is entitled to one. Any such objections on these grounds should be referred to the responsible officer in school or to the Information Policy Section of Education Leeds immediately. This is because there is a 21-day response requirement to state that the request has been received and whether or not the processing will cease as requested. This right does not apply under the following circumstances: -

- If the data subject has already consented to the processing
- The processing is necessary for the performance of a contract
- Processing is necessary to comply with legal obligations (other than contractual)
- Where the processing is necessary to protect the vital interests of the data subject

Right to prevent processing for direct marketing (Section 11)

The third right, about ***direct marketing*** means that the data subject should ideally ***opt in*** for any direct marketing purposes. Small tick boxes in obscure parts of an application form with *"tick here if you do not wish to receive further information*" are no longer considered to be fair under the First Data Protection Principle.

If you need to use such a statement then it should be re-worded to "***tick here if you wish to receive further information***". However, there is a potential sting in the legislative tail, which it is important to understand. ***If parents give personal data to school for one purpose (such as the enrolment of their child) and it is subsequently used to write to parents about some other, different and non-statutory service, this might be caught under the direct marketing rule***.

An example of this might be where school, under a reciprocal arrangement, write to inform parents that a discount in some local garden centre has been secured following the donation of plants or equipment in return. In such cases, there is a risk that schools may be breaching the individual's right to object to direct marketing. Under such circumstances, it is always advisable for school to include on any such correspondence that if no further notices or letters of this nature are desired then parents should indicate this by returning a slip or by writing to a nominated contact in school.

Rights about wholly automated decision making (Section 12)

The fourth right, about ***automated decision-making***, is really targeted at the credit referencing industry. Data subjects can easily be refused credit under automated reference systems with no appeal to a representative of the organisation. Under the Data Protection Act, the data subject can demand a written explanation of how the automated decision was taken and ask for a member of staff to re-assess it.

However, this right will equally apply to any automated decision-making processes that school puts in place. Schools ***must*** therefore ensure that they have adequate procedures in place to explain how any automated decisions are reached and be able to perform the same process manually if asked to do so.

For example, if optical mark readers are used to determine a child's score in a test, then this process of scoring must be explained on receipt of a request from either a pupil at school (if over 12 and able to understand what this particular right means) or from his or her parent. ***Either the pupil or his or her parent also has the right to object to this method of automated scoring and can insist that a re-assessment is undertaken by a member of school staff instead.***

Right to seek compensation for damage or distress (Section 13)

The right to compensation might arise where school has not taken ***reasonable care*** when processing personal data and has caused damage or substantial distress. It may also arise in circumstances where school fails to comply with the rights of an individual, for example, ***subject access requests***.

It should be noted that it does not necessarily have to be the data subject who suffers damage or distress. For example, if a parent following some breach of the Act in connection with his or her child suffers this, they themselves can take action for compensation. Children cannot take action themselves; they must sue by a ***next friend*** (e.g. their parent or guardian).

In any case where damage or distress is claimed, it must be demonstrated that this was due to a contravention of the Act. Damage might result from such things as loss of earnings or benefit or equally from pain or suffering. Loss of reputation would also be covered under this provision. Distress alone is not usually sufficient to justify successful claims unless the distress is substantial and is associated with, for example, psychiatric or other medical conditions. All of these effects must be evidenced, say for example, by a medical certificate or demonstration of loss of earnings or benefit.

Claims for compensation are likely to stand unless it can be proven that school took reasonable care to prevent such damage or distress, for instance, by having a data protection policy and by training its staff in the requirements of the Act.

For the level of damages and fines applicable to breaches of the Data Protection Act 1998, please refer to **Enforcement** later in this guide.

Right to rectify, block, erase or destroy inaccurate personal data (Section 14)

An individual may apply to Court for an order requiring school to rectify, block, erase or destroy their personal data if it is inaccurate. This might also include other personal data which contains an expression of opinion which the Court finds is based on the inaccurate data. Data will be considered inaccurate if it is incorrect or misleading in any matter of fact.

A data subject can also apply for an order if he or she can prove that damage has been suffered through any contravention of the Act, such as processing inaccurate personal data, which entitles him or her to compensation (see **Right to seek compensation for damage or distress (Section 13)**). In either of these cases where the Court considers it to be reasonable,

school can be ordered to notify third parties, to whom the data has been disclosed, of the rectification, blocking, erasure or destruction ordered.

In simple terms, rectification entails making the personal information accurate by removing errors, although it is good practice to be able to demonstrate what the original error was in order to provide an audit trail.

Blocking orders require, for example, that the personal information in question should no longer be disclosed to any or to specified ***recipients***. It may also be useful in the context of the Second Data Protection Principle in order to block processing of personal data for purposes which are inconsistent with the original purpose for which it was collected.

Erasure of personal information appears at first glance to mean the same as destruction in that once either has been carried out, the personal information should no longer exist. However, the difference is to do with the medium on which the information is held.

For example, a sheet of paper on which personal information is held and which contains no other information can be destroyed and this will serve the purpose of ensuring that the personal information no longer exists. However, personal information held on a computer disk might exist alongside other information, the removal of which has not been ordered. In such circumstances, the erasure of the specified personal information serves the purpose of ensuring that it no longer exists whilst the other information remains intact.

It is good-practice to keep a reminder not to collect any information again which has already been the subject of such an order.

Right to ask the Information Commissioner for a ruling about whether the Act has been contravened by School (Section 42)

An individual may choose to request that the Information Commissioner carries out an assessment where he or she feels that they have been directly affected by the processing in question. Such requests do not have to state whether it is suspected that a breach of the Act has occurred although this is often the case, for example, where:

- A data subject is unhappy with the way in which a subject access request was handled or if the request was ignored
- A data subject is not satisfied that school complied with their request that their personal data should not be used for direct marketing purposes

Such assessments commence with the issuing of an ***Information Notice*** by the Commissioner. Such a notice would inform school of the nature of the complaint and ask that certain information be provided in order that the Commissioner may make an assessment as to whether or not a breach has occurred. It must also set out what rights of appeal school have against the complaint, the time-scale for response and the form in which the requested information is to be provided. The Commissioner can issue a warrant for entry into premises in the event that an information notice is ignored. ***It must be noted that failure to comply with any notice issued by the Commissioner is a criminal offence.***

Following the assessment, the Commissioner may, if he finds that a breach has occurred, issue an ***Enforcement Notice.*** This is a statement of action that is required in order to rectify any operational problems identified in the assessment. Again, such a notice must set out what

rights of appeal school has against the notice, the time-scale for response and what action it is required to take in order to ensure that further processing is compliant with the Act. ***Again, such a notice must be complied with as to not do so is a criminal offence.***

Data Sharing

The requirement of the Second Data Protection Principle must be remembered in connection with any proposed data sharing exercise. This states that personal data provided for one purpose cannot be used for another purpose unless the data subject has given permission for the new use or processing.

This will limit the possibility for schools to share data with other organisations in the absence of some over-riding legal authority or obligation. Such legal obligations are often the justification for providing personal information to Education Leeds and the DfES for example. However, the extent of the relevant authority must be clearly understood in order to prevent information being shared, which is not covered.

In general terms, if the data subject has not consented, sharing ***must*** be ***necessary for a statutory function***. It is useful to bear in mind the following points:

- Sharing data between organisations is permitted if the data subject has agreed or if it is necessary to perform a public function.

- The shared use of information must be "***fair***" and in line with the data subject's rights.

When sharing personal data with other external organisations, there are extra things to be considered.

- A record of the disclosure is needed because if inaccurate information is given, we must be able to issue a correction (see **Appendices 1 & 2**).

- If regular exchanges of personal data are planned, an agreement or protocol to define the who, what, where and when of the sharing is essential. It is recommended that schools contact the Information Policy Section for assistance in this respect as information sharing protocols and agreements are very technical documents.

- If school regularly shares data with Education Leeds or Leeds City Council Departments, then a Service Level Agreement or Protocol is also recommended, as this will codify the arrangements and make sure the data sharing is clearly understood by all staff.

- The Police have powers to ***request*** personal data using a "Section 29 Notice" or "DP7 Form" (see **Appendix 3**). The word "request" applies to everyday crime and disorder. See the "**Disclosure of Personal Data**" section.

- Other agencies have powers to ***demand*** personal data. Those most likely to be encountered are: -

    - The Inland Revenue
    - Customs and Excise
    - The Child Support Agency

If any organisation asks for personal data they can only ask about specific individuals. They are not allowed to conduct “fishing expeditions” to look at whole groups of people “just in case”. The request must always be in writing.

The Police and other security agencies have other powers that may be invoked (e.g. the Terrorism Act 2000) that empower them to ***demand*** access to personal data. It is suggested that any requests of this type are immediately referred to the Information Policy Section of Education Leeds or to the responsible officer in school to ensure the notice has been properly constructed and served.

For information, Education Leeds have committed to a number of protocols, which involve the use of pupil information. The most significant of these is with the local area Health Authority and its other partners where information sharing is seen as essential in order to provide more effective local services. All protocols are carefully considered before they are adopted with particular emphasis on the lawfulness of the proposed sharing exercise. In most cases, an actual Information Sharing Agreement is created between the parties sharing information and this includes reference to relevant procedures and considerations in the protocol document itself.

School wishing to know more about protocols to which Education Leeds are party and about specific information sharing agreements already in place are encouraged to contact the Information Policy Section for further information.

Enforcement

The 1984 Act did not include many significant offences but in contrast, the 1998 Act has a number of powerful ones.

First and foremost, school can find itself in court. There are criminal offences, e.g. failing to notify properly (a £5,000 fine) or using personal data for a new and different purpose without asking the data subject first. There are also civil actions that the data subject can take if they feel that school has caused them damage or substantial distress. A civil action could result in heavy damages (there is no defined limit).

However, there are also similar liabilities on each and every member of staff. If a member of staff wilfully disregarded Data Protection rules and, say, gave away personal data to a debt collection agency, that member of staff could find him or herself in court facing a £5,000 fine and then be sued by the data subject as well for extensive damages.

Also, the Information Commissioner can, if he considers that a very serious breach has occurred, enter the offending school premises ***and order school not to use the whole data file until the problem has been corrected.*** Obviously, school will have great difficulty functioning if its main data files (manual or computerised) are closed down and cannot be used.

Fines and Damages

The level of fines and damages are dependent in which Court a case is heard in. For example, if a case is heard in County Court then the maximum fine is £5,000 with no maximum limit for an award of damages. If a case is heard in High Court then both fines and damages are unlimited and the judge may award whatever level is considered appropriate.

As a guide, it is likely that individual claims will be heard in County Court. High Court hearings are unlikely unless an injunction against processing is being sought.

Where an order to take specific action or to cease taking specific action has been granted yet not complied with, this can be treated as a contempt of Court. In such cases, the contemptor can be imprisoned until the contempt has been purged.

Summary

At first sight, Data Protection appears daunting. It need not be. Most of the Principles are just common sense. If they are followed then few problems will arise.

In summary, the Data Protection Act says: -

- The individual – *the* ***data subject*** – has certain rights to privacy.
- The information about any individual must be kept secure and confidential.
- In general, the individual must give school permission to use (***process***) their data.
- There is a new class of "***sensitive personal data***" that is given special protection.
- School cannot use personal data for different or new purposes unless certain strict conditions have been met.
- Personal data cannot be given to external organisations unless certain strict conditions have been met.
- The data subject has a number of new rights regarding Data Protection.

In practice, most staff can observe the requirements of the Data Protection Act 1998 by following some simple operational principles. These are: -

- There must be a good reason for school to hold and process the personal data in question.
- Always make sure the personal data you are handling is correct.
- Remember that much school data is ***sensitive*** and needs extra protection.
- Don't give personal data away to any other organisation or person unless your supervisor or the person responsible for compliance with the Act in school has told you can do so.
- Always follow the rules set out in this guide about getting the data subject's permission to hold their personal details.
- Remember that Data Protection applies to all personal data whether it is held on computer or any type of manual file.

The most important point about Data Protection is that if the data subject, parent, pupil (or whomever), is treated in a manner which is: -

- ***Decent***
- ***Legal***
- ***Honest and***
- ***Truthful***

Their Data Protection rights will almost certainly be protected and school will be well on the way to meeting their obligations under the Data Protection Act 1998.

If you have any queries about Data Protection, first of all talk to your supervisor or Head Teacher. If they are unsure of what to do, the Information Policy Section of Education Leeds is always available to help schools in this respect.

Whatever you do, it is always better to ask than to get things wrong because the consequences can be severe.

Useful Contacts

Paul Taylor, Information Policy Manager,
Education Leeds,
Information Management Team,
10th Floor East,
Merrion House,
Leeds,
LS2 8DT.

Tel. (0113) 2477889
Fax. (01130 2475354
E-mail: educ.info.policy@educationleeds.co.uk
Web: www.educationleeds.co.uk

Jane Sheehan, Information Policy Officer,
Education Leeds,
Information Management Team,
10th Floor East,
Merrion House,
Leeds,
LS2 8DT.

Tel. (0113) 2243615
Fax. (01130 2475354
E-mail: educ.info.policy@educationleeds.co.uk
Web: www.educationleeds.co.uk

Office of the Information Commissioner,
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel. (01625) 545745
Fax. (01625) 524510

E-mail: data@dataprotection.gov.uk
Web: www.dataprotection.gov.uk

Appendix 1

General Guidelines for Notifying Third Parties of Errors in Data

A balance must be struck between the duty to notify corrections in data and the practical limits of operating within the environment of school. While this note includes a discussion in general principles, at the end of the day, it will be up to the individual to exercise their own skill and judgement on whether any particular error must be notified to any or all relevant third parties.

The two key elements of any decision will be

- *When the disclosure took place*
- *How important is the error in the context of the data subject's rights*

An obvious starting point is an error in data where the disclosure occurred before 1 April 2001. School may not have any record of the third party to whom the data was disclosed. In the absence of this information, a correction cannot be issued. However, if the error was truly a life threatening one, school will still have a duty to use its *best endeavours* to trace possible third parties.

Time will be of the essence with errors. An error that is discovered within days of the third party disclosure needs to be corrected within a similar time frame. However, if the same error is discovered 10 years after the disclosure, it may be considered that too long has passed for any action to be needed. This does not mean that after a few years the error can be conveniently forgotten. The question that needs to be answered is, "*could the perpetuation of the error still lead to the data subject suffering any loss in any way?"* If the answer is yes, the correction must be notified.

The importance of the error must be carefully considered. Some errors will be more important than others. For example, misspelling a data subject's name can easily cause confusion and mistakes in identity. However, a minor misspelling of the first name of one of their five children is unlikely to threaten the rights of the data subject. Thus, if the error is considered to be very minor, school may take the view that a correction need not be issued. However, if this decision is taken, *it will be good practice to record that the correction has not been issued.* Don't forget that the Information Commissioner's staff might audit the records.

An error may have a different importance to two or more third parties. It may be inconsequential to one but vital to another. An appreciation of the third party's role and obligations is necessary.

It is recommended that the following types of errors be given high priority for correction.

- Where there is an immediate impact on crime prevention and its investigation
- Data concerned with loan, grant or benefit payments where the data subject may suffer immediate or continuing loss
- Where the data subject's health or safety is at risk

The primary objective is to avoid any case where the data subject may suffer damage or distress. If either of these two possibilities exists, then school should take all reasonable steps to issue a correction to all third parties.

The key element here is *reasonableness*. It is difficult to define but at the end of the day, if the issue ends up in court, this is one of the main tests that the judge will apply: "Did school act reasonably in this case?"

Appendix 2

Recording of Third Party Disclosures

It is useful to have either a database or simple register to record all relevant data about disclosures. It should provide an adequate audit trail and necessary records in the event of a query from the Information Commissioner's Office.

The fields to be contained in the database or register are explained below:

- **Disclosure number**
  A number used to identify ***uniquely*** each recorded disclosure

- **Person dealing with disclosure**
  Name of person dealing with this disclosure

- **Telephone number of person dealing with disclosure**

- **Name of data subject**
  The name of the person to whom the disclosed data relates

- **Address of data subject**
  The address of the person to whom the data relates

- **System name**
  The name of the computer system from where the data originated, e.g. STAR, Personnel Module or other area of SIMS. If no computer system was involved then the name of the area of school making the disclosure should be inserted, e.g. school office, etc.

- **System identifier**
  The record number of the data from the computer system which has been disclosed or if not applicable, any unique identifier such as pay number, Unique Pupil Number etc.

- **Information contained in the disclosure**
  A description of the information provided. This should demonstrate both the extent of the information disclosed (e.g. details of all 13 year olds on school roll) and the level of information disclosed (e.g. name, date of birth, ethnicity)

- **Recipient type**
  The type of organisation to which the data has been disclosed. This could be the Police or a government department, for example.

- **Recipient name**
  The name of the organisation to which data has been disclosed.

- **Recipient contact name**
  The name of the person to whom the disclosed data was sent in the organisation identified above.

- **Recipient's address**
  The address where the disclosed data was sent

- **Authority under which disclosure made**
  The name of the Act of Parliament or other power under which the disclosure was requested, e.g. Section 110, Social Security Administration Act 1992.

- **Date of disclosure**
  The date the disclosure was made

- **Details of any correction made**
  A note of any subsequent corrections that were made to the data in respect of inaccuracies and which were notified to the recipient

- **Date of correction**
  Date the correction was notified

- **Date of subject access request**
  The date that details of this disclosure were included in response to a subject access request.

Appendix 3

Section 29(3) request from West Yorkshire Police

To: ……
Address:……..
……
……..
Postcode:…….

Position Held …….

Data Protection Act 1998, Section 29(3)

I am making enquiries, which are concerned with: —
(a) The prevention or detection of crime:
(b) The apprehension or prosecution of offenders (Delete as appropriate).

Nature of enquiry. ……
The information sought is needed to:……
……
…..……

and possibly for other crime enquiries.

I can confirm that the personal data requested are required for the purpose(s) stated above and failure to provide information will, in my view, be likely to prejudice that/those purpose(s).

Signed;…… Rank: …….

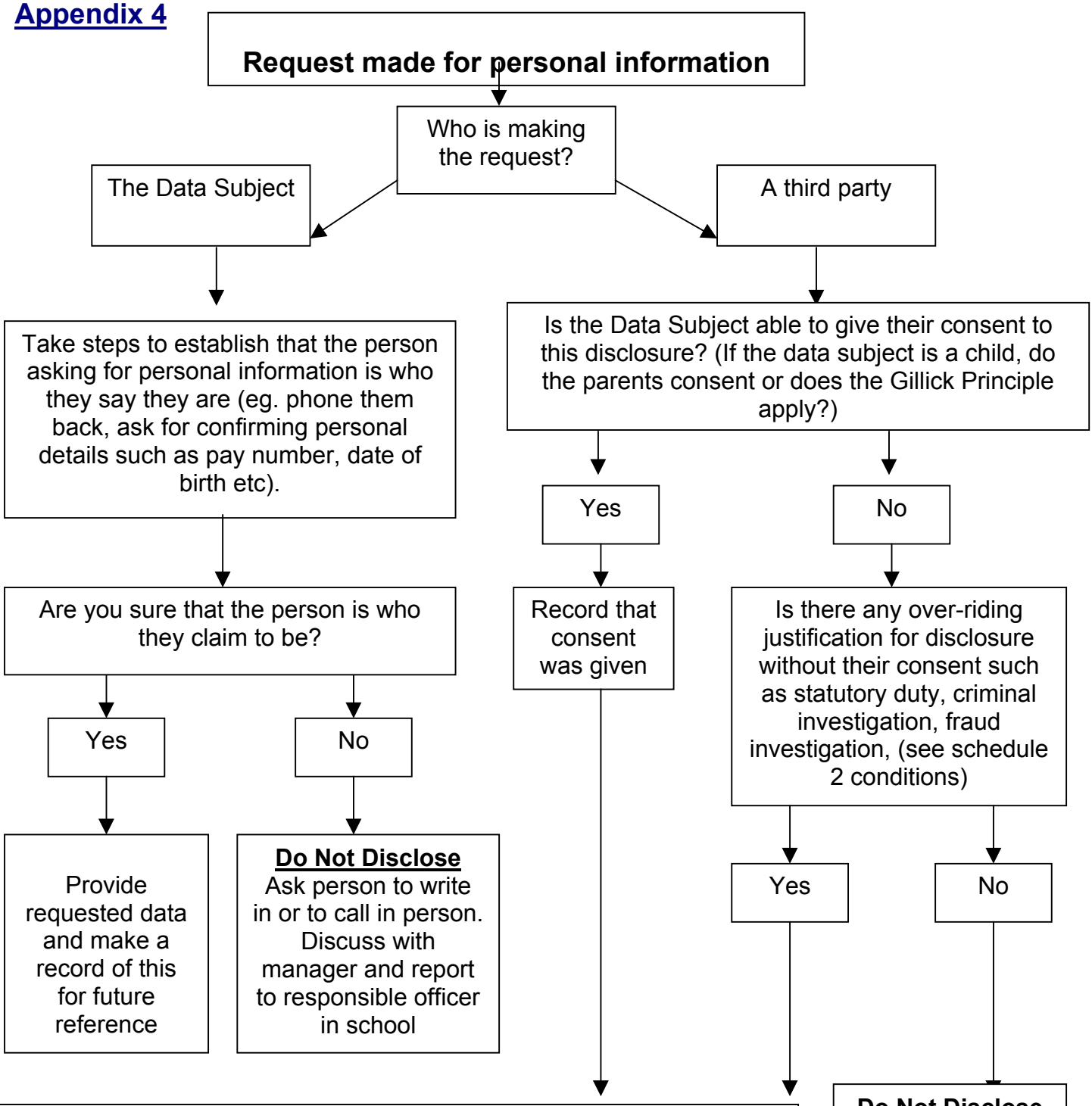
Name…… Date: …….
(BLOCK CAPITALS)

Police Station……

Countersigned: …… Rank: ……
(To be countersigned by senior officer when reason for request cannot be given)
D.P.7

This last section will not be used very often because in most cases the Police will give a reason. However, there may be instances where this is not possible because to do so might constitute what is known as a “tip-off” (i.e. the person who is the subject of the inquiry may find out and this would prejudice the investigation). There may also be instances where the Police cannot tell us why the information is required because their investigation is to do with National Security.

Appendix 4



3.1. Do not disclose over the telephone. Ask the third party to write or fax stating: -

a). Under what authority they are requesting the information, e.g. which Act of Parliament
b). What their organisation's relationship is in respect of the Act stated at a).
c). Why the information is required

Record that the disclosure has been made, for future reference.

Appendix 5

Code of Practice for Use of Images

1) Introduction

a) This Code of Practice provides a framework for lawful use of photographic and video images in order to comply with the requirements of the Data Protection Act 1998 and Human Rights Act 1998 (in particular, Article 8). The code has two main aims:

i) To ensure that where necessary, consent has been given prior to the taking and use of images on school premises, particularly where these show pupils.

ii) To ensure that such images are used in a manner respectful of the eight Data Protection Principles and also of the rights conferred to individuals under these Acts.

b) The code deals with use of images for both business purposes (such as inclusion in publications or promotional materials) and personal use (such as images captured by parents attending a school play).

c) A sample "**Photo Use Form**" is attached for obtaining consent before images are captured in ***any format*** for business purposes.

2) Responsibilities – Business Use of Images

a) Examples of internal business use include images required for carrying out statutory duties, (for example, health and safety). Where this is the case, the statutory authority should be specified on the photo use form including the name and section of the Act or regulations in question. Where a statutory authority is being exercised, consent is not usually required. Staff newsletters, articles on the Intranet or Internet, marketing materials and newspaper items also fall into this category along with many others.

b) Examples of external business use include documents, leaflets, brochures or displays made available to the public, newspapers or publication on a website. It is also possible that a statutory authority may be exercised by an external body and again, this should be specified on the photo use form including the name and section of the Act or regulations in question. Where a statutory authority is being exercised, consent is not usually required.

c) The person wishing to capture images is responsible for obtaining consent. This applies whether they are a member of school staff, an Education Leeds or Leeds City Council Officer or a representative of any other external organisation (e.g. from the press).

d) Consent may not be required for staff photographs which are ***necessary*** for employment purposes or for the performance of a contract to which the employee is a party. However, written consent is necessary in the event of external publication, particularly if this is to be on the Internet.

e) Images are required to be accurate and up to date where these are to be continually used as a “live” source. However, this does not apply to images captured only to record a moment in time.

   i) This principle also has implications for consent in that this too needs to be accurate and up to date. Consent should therefore be time-limited to approximately 12 months. Beyond this, circumstances may have changed and consent may no longer be available. It is the responsibility of the person or organisation seeking to continue use of the images to renew consent.

f) Processing beyond a reasonable time limit where no accuracy checks have been undertaken risks causing damage or distress. Such processing exposes the processor to risk of liability for fines and damages.

g) Where images are to appear in subsequent publications, it is imperative to ensure that the persons giving consent are aware of this. Under such circumstances, consent must be in writing and in relation to children under 12 (see item 6, “**Definitions**”) this must be from one of their parents. For children over 12, even if they are of sufficient understanding to be able to give consent in writing for themselves, parents should be informed as a matter of courtesy.

h) Images originally captured for internal business purposes must not be placed in the public domain without specific written consent from the subject(s).

i) School may choose to obtain consent on behalf of any person wishing to capture images. However, it remains the responsibility of the person wishing to do this to ensure that consent has been obtained in advance and in accordance with the “Fair Processing Code” (see item 6, Definitions).

j) The name of the organisation seeking to use the image(s) should be made very clear on the form including contact details such as name and address.

k) The actual purpose of the images should be as specific as possible on the consent form (for example, in order to publicise a specific initiative and by what method). This should also take into account any caption that might be added to the photo or the context in which it is to be set (for example, to promote healthy schools). Education Leeds do not advise the inclusion of a child’s full name along with published photographs as this may lead to vulnerability. If a name is to be included then this should be restricted to christian name only.

l) If the images are to be further disclosed (other than made public) then details of either individual recipients or groups of recipients should be recorded. For example, if Education Leeds takes images on school premises that will be sent to the DfES, then this should be made clear. However, if images were to be subsequently passed to prospective contractors then it would be sufficient to state this rather than to name all possible contractors to whom the images may be released.

m) Any other information in order to ensure fairness should be provided. This might include details of who to contact in order to exercise rights such as the right to subject access (which is the right to have a copy of information held about you by an organisation).

n) The person holding the images, once captured with consent, must be respectful of the Data Protection Principles and also the rights conferred to individuals under the Act.

3) Responsibilities – Personal Use of Images

a) The Data Protection Act does not regulate personal use of images (such as those captured by parents attending a school play). However, where such images are captured on school premises it is important that it is made clear in advance whether or not the capturing of images is to be permitted.

i) If a school play is to have an audience of parents it is likely that some of them may wish to either take photographs or make video recordings of their children taking part. It is also possible that other parents will not wish their children to be photographed or recorded at all.

ii) In order to avoid such conflict, school can choose to state in advance whether or not the capturing of images is to be permitted. Parents can then decide in advance whether or not to allow their child to participate in light of the fact that recording and photography will be taking place.

iii) Alternatively, school may choose to prohibit personal photography and recording altogether yet make a recording of the play and to take photographs themselves which can be made available to parents later. However, as this will be business related (even if provided for free) then written consent must be obtained in advance.

iv) ***Note: Where image capturing on the part of parents is permitted, a warning should be provided emphasising the danger of placing such images on personal web sites. There is a real risk that such images could be used to target victims with criminal activity****.*

b) The Data Protection Act cannot govern use of images captured in public places. For example if a school party are attending a museum and images of some of the party are captured in incidental shots taken by other visitors, this is unavoidable. Under such circumstances it is unreasonable to expect consent to be obtained before images are captured.

i) There will be circumstances where it is impossible to obtain consent. A proportionate approach should be taken here. Many people, including public figures and people attending events and ceremonies, will have no objection to their image being published. However, it may be appropriate for school to forewarn attendees that they may have their photograph taken for publication purposes. If an attendee then objects, school can either ensure that the person is not included in the photograph or take steps to remove them from the final image (by cropping or other editing technique).

4) Considerations Relating to the Data Protection Principles

a) The Third Principle requires that personal data be adequate, relevant yet not excessive. In the context of image capture, this means that images should be proportionate to the purpose stated and should not go beyond that.

b) Images should not be kept for longer than is necessary according to the Fifth Principle. Hence, once the images have reached the end of their useful life (that is to say, when they are no longer required for their original purpose) they should be securely disposed of or alternatively, submitted to the local Archive Service.

c) The rights of individuals must be respected in connection with use of their images (see item 5) below).

d) Where consent to use images in the public domain is not held, adequate security must be put in place to ensure that images are not inadvertently disclosed to persons that should not have access. In cases where digital images are kept in computerised format then these should be afforded adequate technical security. Where images are held in paper or video format then the security surrounding them must be proportionate to the subject matter. For example, if a photograph showing injuries sustained by a pupil is held then this should be kept more secure because it contains sensitive personal information.

e) ***The Eighth Principle states that personal information shall not be transferred beyond the European Economic Area without adequate protection or explicit consent. This has implications for images placed in the Internet, which is by definition worldwide. It is especially important to ensure that the intention to make images available over the Internet is clearly stated on the consent form and that written consent is sought.***

5) Considerations Relating to Rights

It is particularly important to respect the rights conferred to individuals under both the Data Protection Act 1998 and Human Rights Act 1998. The main considerations are set out below.

a) The right to be told that your personal information is being processed has been covered extensively already in the areas dealing with consent.

b) The right not to suffer damage or distress as a result of the processing of personal information has implications for images. For example, the London Borough of Newham was ordered to pay £5,000 in damages and £50,000 towards legal costs following use of a child's photograph without consent on the front of its AIDS strategy publication. The child in question did not have AIDS although was subsequently avoided by friends because they assumed otherwise.

c) The right to withdraw consent also has significant implications for the use of images, particularly where these are to be used in marketing material. If consent to use images is withdrawn then this might mean reproduction of materials without the image in question. This could be very costly, although fines as a result of non-compliance could

be costly too. It is always better to provide an opportunity for the data subject to see the photograph beforehand to ensure that they still consent to its use in the intended manner. The right to subject access is one frequently exercised. Images held by an organisation must also be considered for release following such a request.

d) Article 8 of the Human Rights Act confers the right to private, family life and correspondence. This also states that a public authority (such as a school) must not interfere with this right except in specific and limited circumstances. An image can interfere with this right, particularly if it is intrusive or displays something that the subject prefers to keep private.

6) Definitions

a) A photograph or video image may be considered "**personal data**" if an individual can be identified from this and other information which is or is likely to be held or obtained. This would include a caption showing names at the foot of a photograph or a caption in a publication adjacent to a photograph. This also includes situations whereby relatives, friends or others can identify someone in an image.

b) "**Fair Processing**" requires that certain information must be provided at the time consent is sought in order to ensure that the processing is fair. This information includes the name of the organisation wishing to process; the purpose for which the information will be processed; to whom the information may be further disclosed and any other information necessary to ensure fairness.

c) Children can exercise their own data protection rights once they are old enough to understand the implications of what they are being asked. It is generally acknowledged that the usual age where this becomes the case is around 12 years old. However, there may be circumstances where a child of 12 is not of sufficient understanding (for example, because of special needs). It is reasonable for one of the child's teachers to make an assessment as to how well a the child understands given that they will probably have first hand knowledge of this.

Indeed, there is case law that establishes that children should be able to decide such things for themselves at or around the age if 12, (Gillick v. West Norfolk and Wisbech Health Authority). This is generally referred to as the "Gillick Principle".

Appendix 5a

Photographs of Children – Parental Consent Form

Your child has been selected for inclusion in photographs which the following organisation wishes to take on the date(s) shown:

Organisation: ……..…

Date photographs to be taken: ……..…...

The purpose(s) for which the photographs are to be taken are:…….……

..……..…

These will be published in the following places (must clearly state "internet address" if it is intended to publish via this medium):…….……..…..

……..

May we include your child's first name with this photograph?.... ..... **YES / NO** (delete as appropriate)
Note: Education Leeds strongly recommends that names are not used in association with photographs or that where absolutely necessary this is limited to first name only.

If you have any queries regarding use of these photographs or change your mind then please contact the above organisation at the following address:
……..

……..

Declaration

I grant permission for photographs of my child(ren) to be used in printed and electronic (*delete as appropriate*) publicity materials generated by the organisation named above. I acknowledge that the photographs will only be used for the purpose(s) stated and that I have a right to change my mind.

Name of Child ……..

School Attended ……..

School year …….

Your Name ……..

Signature …….

Child's Signature (if over 12 years) …….. Date _ _ / _ _ / _ _

Appendix 6

Statutory Instruments Affecting Data Protection

The Telecommunications (Data Protection and Privacy) Regulations 1999
Statutory Instrument 1999 No. 2093

The Data Protection Act 1998 (Commencement) Order 2000
Statutory Instrument 2000 No. 183 (C.4)

The Data Protection (Corporate Finance Exemption) Order 2000
Statutory Instrument 2000 No. 184

The Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 Statutory Instrument 2000 No. 185

The Data Protection (Functions of Designated Authority) Order 2000
Statutory Instrument 2000 No. 186

The Data Protection (Fees under section 19(7)) Regulations 2000
Statutory Instrument 2000 No. 187

The Data Protection (Notification and Notification Fees) Regulations 2000
Statutory Instrument 2000 No. 188

The Data Protection Tribunal (Enforcement Appeals) Rules 2000
Statutory Instrument 2000 No. 189

The Data Protection (International Co-operation) Order 2000
Statutory Instrument 2000 No. 190

The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 Statutory Instrument 2000 No. 191

The Data Protection Tribunal (National Security Appeals) Rules 2000
Statutory Instrument 2000 No. 206

The Data Protection (Subject Access Modification) (Health) Order 2000
Statutory Instrument 2000 No. 413

The Data Protection (Subject Access Modification) (Education) Order 2000
Statutory Instrument 2000 No. 414

The Data Protection (Subject Access Modification) (Social Work) Order 2000 Statutory Instrument 2000 No. 415

The Data Protection (Crown Appointments) Order 2000
Statutory Instrument 2000 No. 416

The Data Protection (Processing of Sensitive Personal Data) Order 2000
Statutory Instrument 2000 No. 417

The Data Protection (Designated Codes of Practice) Order 2000
Statutory Instrument 2000 No. 418 – REVOKED as of 27th July 2000 by: -

The Data Protection (Designated Codes of Practice) (No.2) Order 2000
Statutory Instrument 2000 No. 1864

The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000
Statutory Instrument 2000 No. 419

The Data Protection (Miscellaneous Subject Access Exemptions)
(Amendment) Order 2000 Statutory Instrument 2000 No. 1865

Statutory Instrument 2000, No.297, The Education (Pupil Information) (England)
Regulations

Appendix 7

Glossary of Terms

Accessible Record	A health record created by a health professional, a school educational record or a public record relevant to local authority housing or social services Special rules apply to these records as they are subject to secondary legislation
Audit Trail	To determine whether activities involving the processing of personal data are carried out in accordance with an organisation's data protection policies and procedures, and whether this processing meets the requirements of the Data Protection Act 1998.
Automated Decision-Making	There exists software which can process application forms for credit, or even job applications and which can make decisions automatically, without the need for human intervention.
CCTV Code of Practice	Guidelines set out by the Information Commissioner on the operation of CCTV systems. It sets out the standards which must be met if the requirements of the Data Protection Act 1998 are to be complied with.
Computer Files	Any computerised record whether on mainframe computers, network or stand-alone PC
Community Finding	The European Commission is considering the data protection laws of a number of non-EU countries to ascertain whether those states provide adequate protection for personal data transferred from the EU. Countries that are considered to do so will be subject to a 'Community Finding' allowing EU data controllers to transfer personal data to those states without further consideration of the adequacy of the protection provided for the data transferred. Therefore, UK data controllers will be able to transfer personal data to any country subject to a 'Community Finding' and comply with the 8th Principle on that basis.
Confidentiality	An obligation of confidence arises between 2 parties, and gives the person who imparted the information the right not

to have that information used for other purposes or disclosed unless:-

a) they give consent

b) there is a legal compulsion

c) there is a duty to the public

Covert Surveillance

Surveillance is defined as 'covert' if , and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place". It is the view of the Commissioner that the surveillance should be regarded as covert if the effect is that persons are unaware that it is being carried out. It should not be defined on the basis of whether it is the intention of those carrying out the surveillance to ensure that the persons are unaware. It is whether the person is in fact aware that is important. This is the approach taken in the Data Protection Act 1998 which requires the provision of prior information to data subjects to make processing of their personal data fair.

Data

Information which is: -

a) Being processed by means of equipment operating automatically in response to instructions given for that purpose; for example a computer, camera, optical mark reader or tape recorder.

b) Is recorded with the intention that it should be processed by means of such equipment described above;

c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or

d) Does not fall within paragraph a), b) or c) but forms part of an “accessible record”

e) Is recorded information held by a public authority and does not fall within a to d above.

Data Controller

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 [Data Protection Act 1998].

Note: The data controller is usually a company or organisation

Data Processor	Any person or organisation (other than an employee of the data controller) who processes personal data on behalf of the data controller
Data Protection Principles	Anyone processing personal data must comply with the eight enforceable principles of good practice:- a) fairly and lawfully processed; b) processed for limited purposes; c) adequate, relevant and not excessive; d) accurate; e) not kept longer than necessary; f) processed in accordance with the data subject's rights; g) secure; h) not transferred to countries without adequate protection
Data Subject	An individual about whom data is held
Demand	To claim formally; lay legal claim to
Direct Marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals

Disclosure	Enforced or voluntary publication of information
Educational Record	Any record held by a school in connection with a child's education **(as defined by Schedule 11 of the Act).**
Enforcement Notice	Under section 10 of the Data Protection Act, 1998, the Information Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Act, 1998. Such steps could include correcting the data, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether. The Commissioner exercises this power by providing a written notice, called an "enforcement notice", to the data controller or data processor. It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.
European Economic Area (EEA)	All the member states of the European Union plus certain other countries with associate status. Currently the EEA members are: Austria; Belgium; Denmark; Finland; France; Germany; Greece; Holland; Iceland; Ireland; Italy; Liechtenstein; Luxembourg; Norway; Portugal; Spain; Sweden and the United Kingdom
Explicit	The indication of consent demonstrated by a signature or some other positive indication
Explicit Prior Informed Consent	An individual understands what they are consenting to and indicates consent by a signature or some other positive indication before processing starts
Expectation of Privacy	Where individuals might ordinarily expect to have a high level of privacy such as in toilet facilities or in their home or correspondence.
Fair	In a proper or legal manner

Fair Processing Notice

A notice (or declaration) usually at the foot of a form setting out specific information in order to satisfy the fair processing code. This notice should include:

The name of the data controller (i.e. school name);

The purpose of the processing (e.g. for organising a school trip);

Details of non-obvious processing (such as disclosure to another organisation);

Any other information required to ensure that the processing is fair. For example, information that will enable the data subject to exercise his or her rights, such as the right of subject access.

Human Rights Act 1998

This came into force on 2nd October 2000. Article 8 is relevant to the Data Protection Act which states that everyone has the right to respect for his private and family life, his home and his correspondence.

Identity Theft

A crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, usually for economic gain.

Information Commissioner

The person appointed by the Government to administer the provisions of the Data Protection Act 1998 and the Freedom of Information Act 2000. Since December 2002 the Commissioner is Richard Thomas. This post was previously known as Data Protection Commissioner in respect of the 1998 Act and Data Protection Registrar under the 1984 Act

Information Notice

Under section 12 of the Data Protection Act, 1998, the Information Commissioner may require any person to provide him with whatever information the Commissioner needs to carry out his functions, such as to pursue an investigation. The Commissioner exercises this power by providing a written notice, called an "information notice", to the person.

Manual Files

Files which are paper based or on any format other than computerised (e.g. microfiche, video or audio or even on a post-it note).

National Security

If it is necessary for the purpose of safeguarding national

	security any data may be released.
Necessary	Processing which is absolutely essential
Next Friend	Parent, guardian or other legally appointed representative of a child who is taking legal action on their behalf.
Notify	Data Controllers need to notify the Commissioner of the purpose of their processing, the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register.
Notification	This is the process by which a data controller's details are added to the register. The Data Protection Act 1998 requires every data controller who is processing personal data to notify unless they are exempt. Data Controllers have a single register entry and notifications are renewable annually.
Opt in	To chose to participate in something.
Personal Data	Data that relates to a living individual who can be identified: **a)** From that data; or **b)** From that data and other information which is in the possession of, or is likely to come into the possession of the data controller; and **c)** Includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual [Data Protection Act 1998] **Note**: This includes audio and video formats as well as written and computerised data.
Personal Privacy	The right of the individual to be protected against intrusion into their personal life by direct physical means or by publication of information
Prior Informed Consent	An individual understands what they are consenting to and agrees in advance before processing starts

Processing In relation to data this is:

Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

a) Organisation, adaptation or alteration of the information or data;

b) Retrieval, consultation or use of the information or data;

c) Disclosure of the information or data by transmission, dissemination or otherwise making available; or

d) Alignment, combination, blocking, erasure or destruction of the information or data [Data Protection Act 1998]

Purpose An anticipated outcome that is intended or guides your planned actions

Reasonable Care The care that a reasonable person would exercise under the circumstances

Recipient Any person to whom personal data is disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of the data processor) to whom it is disclosed in the course of processing the data for the data controller, but not including any person to whom disclosure is, or may be, made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law

Regulation of Investigatory Powers Act 2000 RIPA controls and regulates covert surveillance, and other means of gathering information, such as intercepting communications

Relevant Filing System

Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. For example, a filing cabinet with drawers arranged A to Z containing staff records in folders arranged in alphabetical order is regarded as a relevant filing system.

Relevant

Having a bearing on or connection with the subject at issue.

Request

To ask for.

Rights

Legal entitlements.

Safe Harbour

The United States takes a different approach to privacy from that taken by the European Union. To bridge these different privacy approaches the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbour" framework. This is a way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbour ensures that EU organisations know that US companies provide “adequate” privacy protection, as defined by the Directive.

Section 29

This allows the release of personal data to the relevant authorities for the purposes of:-

a) the prevention or detection of crime,
b) the apprehension or prosecution of offenders, or
c) the assessment or collection of any tax or duty or of any imposition of a similar nature

Section 55

This section defines criminal offences in relation to unlawful obtaining and unlawful disclosure of personal information.

Sensitive Personal Data

Personal data consisting of information as to:-

a) Racial or ethnic origin

b) Political opinion

c) Religious or other beliefs

d) Trade union membership

e) Health

f) Sex life

g) Criminal proceeds or convictions

Statutory Instrument

Legislation enacted by the UK Parliament and delegated legislation

Subject Access

The Data Protection Act allows individuals to find out what information is held about themselves on computerised, paper based and other types of records. This is known as the right of subject access.

Subject Access Request

A request by individuals to find out what information is held about themselves.

Third party

In relation to personal data, any person other than:

a) The data subject;

b) The data controller; or

c) Any data processor or other person authorised to process data for the data controller or processor

Appendix 8

Data Security Questionnaire to Data Processor		
Organisational Security	**Method / Evidence Required**	**Comments**
4. General		
1. Has your organisation put a data protection policy in place?	Copy of policy	
2. How has this been implemented?	Please describe method	
3. How do you ensure the reliability of staff with access to data?	Details of adopted procedures	
4. Do all staff with access to data receive adequate training in data protection?	Copy of training materials	
5. Can you demonstrate that a breach of data protection policy is a disciplinary offence?	Copy of policy or employment contract	
6. Are organisational measures in place to restrict staff without authority to the data?	Method of restriction	
7. Are you using a subcontractor(s) as part of this contract?	Name of subcontractor(s)	
8. If the answer to (7) is yes; are any provisions in place with this subcontractor to ensure that data security can be guaranteed where they have access to school data?	Copy of guarantees in respect of data	
Technical Security		
9. Are security measures such as encryption used to protect sensitive personal data?	Details of security	
10. Are technical measures in place to restrict access to systems holding personal data, such as passwords and access controls?	Details of access controls	

11. Are technical measures in place to secure data during transit?	Details of method of protection	
12. If you are using a subcontractor for this contract, have they got adequate technical measures in place? Please ensure that they complete a questionnaire of their own.	Details of technical security used by subcontractor.	
Physical Security		
13. Are the premises on which the data is to be held secure?	Details of security	
14. Are the premises subject to 24-hour security such as CCTV?	Details of security	
15. Is the data provided by school held in a secured area within the premises?	Details of security	
16. If the data provided by school is held on removable disc, is this kept in a locked receptacle when not in use?	Storage details	
16a. What level of security is provided for desks and filing cabinets, which might contain prints from this data set?	Details of security	
17. What will be the method of disposal for personal data when the development of the project has been completed?	Method of disposal	
18. Is obsolete hardware and software from which data could be recovered disposed of securely?	Method of disposal	
Encryption If encryption is used:		
19. Has the encryption code been tested?	Documentation	
20. Is mature encryption software used?	Documentation from supplier	

21. Have any problems been reported with this encryption method?	Details of known problems	
Other Issues		
22. Do you carry sufficient insurance cover in the event of liability incurred in respect of a breach of the Data Protection Act 1998?	Details of insurance cover	
23. Will any data be transferred outside of the EEA?	Details of countries to which data may be transferred	
24. Does anyone at your organisation have responsibility for data protection compliance and if so, can this person be contacted to assist us in the event of a subject access request made under Section 7 of the Act?	Name of person responsible	

Appendix 9

Leeds LEA School Notification Template

Purposes:

1. **Education** – Administering of education and training (e.g. registration, monitoring and reporting, calculation and publication of exam results, provision of references). Provision of education and training (e.g. planning and control or curricula and exams, commissioning, validating and producing educational materials, arrangement of work experience placements). Preparation of DfES returns.

   Subjects

   Students and pupils
   Staff, including volunteers, agents, temporary and casual workers
   Relatives, guardians and associates of the data subject
   Complainants, correspondents and enquirers
   Advisers, consultants and other professional experts

   Classes

   Student records
   Religious or other beliefs of a similar nature
   Racial or ethnic origin
   Physical or mental health or condition
   Personal details
   Goods or services provided
   Financial details
   Family, lifestyle and social circumstances
   Employment details
   Education and training details
   Disciplinary records

   Recipients

   Voluntary and charitable organisations
   Suppliers, providers of goods or services
   Relatives, guardians or other persons associated with the data subject
   School boards, school staff, board of governors
   Local Government
   Healthcare, social and welfare advisers or practitioners
   Employees and agents of the data controller
   Education, training establishments and examining bodies
   DfES
   Central Government
   Data subjects themselves
   Current, past or prospective employers of the data subject

Careers service
Survey & Research Organisations

Transfers

Worldwide

2. **Schools administration** – Administration and management of school property. Planning and administration of repair and maintenance, access, security and safety arrangements. Office administration (including office directories, e-mail, word processing, dealing with enquiries and complaints). Administration in connection with board of governors etc. The administration of supplier records relating to goods, orders, services and accounts provided to the school.

Subjects

Suppliers
Students and pupils
Staff including volunteers, agents, temporary and casual workers
Relatives, guardians and associates of the data subject
Governors
Complainants, correspondents and enquirers
Business or other contacts
Advisers, consultants and other professional experts
Members of the public whose images may be captured on CCTV
Offenders and suspected offenders

Classes

Personal details
Financial details
Employment details
Education and training details
Goods and services provided
Offences (including alleged offences)

Recipients

Suppliers, providers of goods or services
School boards, school staff, board of governors
Relatives, guardians or other persons associated with the data subject
Local government
Central Government
Financial organisations and advisers
Employees and agents of the data controller
Data subjects themselves
Courts, tribunals
Police forces
Survey and research organisations

Transfers

Worldwide

3. **Educational support and ancillary purposes** – To include processing for purposes supplementary to the provision of education and training. Administration and provision of health care services. Administration and provision of welfare and pastoral services. Administration and provision of library services (including membership records, loan/hire records, information and databank administration). Careers guidance. Planning and administration of events (e.g. social, sports, school trips etc.). Organisation of parent-teachers and other associations and events involving parents/guardians of pupils. Organisation of alumni and other associations and events involving former pupils and students

Subjects

Welfare and pastoral professionals and advisors
Suppliers of goods and services
Students and pupils
Staff including volunteers, agents, temporary and casual workers
Relatives, guardians and associates of the data subject
Health professionals
Governors
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts

Classes

Student records
Sexual life
Religious or other beliefs of a similar nature
Racial or ethnic origin
Physical or mental health or condition
Personal details
Offences (including alleged offences)
Goods or services provided
Financial details
Family, lifestyle and social circumstances
Employment details
Education and training details
Disciplinary records

Recipients

Suppliers, providers of goods or services
Relatives, guardians or other persons associated with the data subject
School boards, school staff, boards of governors
Professional representatives and advisors
Police forces
Local government
Healthcare, social and welfare advisers or practitioners
Financial organisations and advisers
Employees and agents of the data controller
Education, training establishments and examining bodies

Data subjects themselves
Current, past or prospective employers of the data subject
Courts, tribunals
Careers service
Survey and research organisations

Transfers

Worldwide

4. **Staff, agent and contractor administration** – The administration of prospective, current and past employees including self-employed, contract personnel, temporary staff or voluntary workers. Planning and management of staff workload and/or business activities. Administration of agents or other intermediaries. Vetting checks. Staff training. Occupational health services. Disciplinary matters, industrial tribunals etc

Subjects

Suppliers
Staff including volunteers, agents, temporary and casual workers
Relatives, guardians and associates of the data subject
Previous and prospective employers of the data subject and other referees
Agents and contractors
Advisers, consultants and other professional experts

Classes

Trade union membership
Racial or ethnic origin
Physical or mental health or condition
Personal details
Offences (including alleged offences)
Goods or services provided
Financial details
Family, lifestyle and social circumstances
Employment details
Education and training details

Recipients

Trade unions and staff associations
Suppliers, providers of goods or services
Relatives, guardians or other persons associated with the data subject
Recipients of school services
Police forces
Local government
Legal representatives
Healthcare, social and welfare advisers or practitioners
Financial organisations and advisers
Employment and recruitment agencies
Employees and agents of the data controller
Education, training establishments and examining bodies
Data subjects themselves
Current, past or prospective employers of the data subject
Courts, tribunals
Central Government

Careers services
Survey & research organisations

Transfers

Worldwide

5. **Advertising. Marketing, public relations, general advice services -** Advertisement, marketing and promotion of the school by direct marketing and other means. The provision of general information and advice to members of the public about the school and the services it offers. Identification of potential donors. Funding by direct marketing and other methods.

Subjects

Students and pupils
Staff including volunteers, agents, temporary and casual workers
Relatives, guardians and associates of the data subject
Persons who may be the subject of enquiry/press release/promotional exercise
Donors and potential donors
Complainants, correspondents and enquirers
Advisers, consultants and other professional experts
Authors, publishers, editors, artists and other creators

Classes

Personal details
Lifestyle and social circumstances
Financial details
Employment details
Education and training details

Recipients

The media
Suppliers, providers of goods or services
School boards, school staff, board of governors
Relatives, guardians or other persons associated with the data subject
Employees and agents of the data controller
Data subjects themselves
Persons making enquiries and complaints
Survey and research organisations

Transfers

Worldwide

Appendix 10

Frequently Asked Questions

We have attempted to pre-empt common questions raised by schools in this appendix. These have been grouped into areas representing the services of Education Leeds and also to everyday school business.

General School Business

Q. A parent has approached school for a list of names and addresses in order to send out invitations to their child's birthday party. Can I release this information?

A. No. School has one of two options. Either it can refuse to provide the information or it can offer to pass on invitations to the children in question at school.

Q. A company has approached school with an educational service they wish to market to parents. They have asked for a list of names, addresses and telephone numbers of parents with children at school so they can do this. The service is very good and would benefit the children's education. Can I provide these details?

A. No. Even though the service might be beneficial, school cannot hand over these details. There are strict rules about direct marketing and school could be contributing to an infringement of a person's right to object. This could lead to fines and damages against school. Also, the disclosure would be inconsistent with the second principle in that these details are held for school administration purposes and not for direct marketing. School's notification entry probably wouldn't cover such a disclosure either. The same applies if school were to consider distributing leaflets on behalf of the company. However, making a supply of leaflets available in reception for parents to pick up if they wish is acceptable.

Q. The Police have contacted school over the telephone asking for personal information about one of our pupils. Can I give this to them?

A. Not automatically, there are things to consider. If possible, ask the Police to put their request in writing (using their DP7 form) and to fax it to school. This should state whether a specific crime is being investigated. If so and if the investigation would be seriously hindered if school didn't provide the information, school may disclose the information. If no specific crime is being investigated then school should not provide the information.

Even if a Police Officer insists on disclosure over the phone, it is just as quick to send a fax. If there really is no alternative due to the urgency of the matter (for example, if someone is in a life threatening situation), then take the Officer's details and the telephone number of the station from which he is calling and call him back to verify that he is who he says he is before disclosing the requested information.

Make a note of the disclosure in accordance with the guidelines set out in **appendix 3**.

Q. The school nurse has identified that a pupil has a medical condition and wishes to contact the parents about this. Can I provide the contact details?

A. If this has been discovered in the course of the nurse's duties in school then yes. However, the information disclosed to the nurse should be the minimum required in order to make contact. A note of the disclosure should also be made in accordance with the guidance set out in **Appendix 3**.

This course of action is appropriate in connection with any disclosure to an official where they have a legitimate involvement with the pupil. This might include Education Welfare Officers, Social Workers and Health Officials. Always make sure that you see some form of identification to verify that the person is who they say they are and record what this is together with the relevant reference or ID number.

Q. A newspaper wishes to photograph children in school in connection with a story they are running. Is this acceptable if no names are associated with the picture?

A. No, not without written consent from parents if the children are under 12. Even if the children are over 12 and able to give written consent, the photographs should not be permitted until there has been an opportunity to inform parents that this is going to happen. This is important because there may well be legitimate reasons of which the child is unaware that means a photograph showing their child is not a good idea.

Even if no names are associated with a photograph, children can still be identified. Consider an estranged parent from whom the family have fled because of violence. If the parent sees the photograph, it is likely that their child will be instantly recognisable and thus they will know which school is attended and the general location of the family. This could have serious consequences both for the family in that they might be placed at risk of danger and also for school in terms of liability if the disclosure causes damage or distress.

Q. School are running a trip including an overnight stay. We want to ask parents to complete a form to apply for a place for their child. This form will ask about any health problems in order that we may take the necessary precautions. Do we need to have a declaration on the form?

A. Yes. On any form where you are seeking personal information (whether or not it is sensitive), you must have a "***fair processing notice***". This should provide the name of the school; why the information is required; to whom the information collected might be further disclosed (for example to the coach company with whom travel arrangements have been made) and any other information to ensure that the processing is fair (for example, about any relevant rights).

If the form includes sensitive personal information then it is necessary to also obtain a signature to demonstrate explicit consent. The only exception to this which school are likely to encounter is where a form asks for sensitive personal information in connection with a statutory duty. Under such circumstances a signature is not required although the fair processing notice must still be provided, stating the statutory power

being exercised. For example, it is a statutory requirement that certain health and safety forms be completed following an accident in school and these may contain details of injury (in other words, matters of health). Such forms need only state the statutory power being exercised and the nature of the processing involved, they do not need a signature to demonstrate that consent has been obtained. It is often the case however that a signature is included to verify the authenticity of the information being submitted.

Q. Our Information Technology teacher wishes to place on the internet photographs of some of the children who have helped design school's website. Is this ok?

A. No, not without written consent from parents if the children are under 12. Even if the children are over 12 and able to give written consent, the photographs should not be permitted until there has been an opportunity to inform parents that this is going to happen. This is important because there may well be legitimate reasons of which the child is unaware that means a photograph showing the child is not a good idea. Written consent is especially important in this case because, as the Internet is worldwide by definition, any personal information on it will go beyond the European Economic Area (EEA). The **Eighth Principle** makes it clear that this cannot happen without consent or adequate protection. (See also the earlier example regarding newspaper photographs. These may well be reproduced on the Internet so should be treated identically).

Q. We have received a request from a parent's solicitor asking for sight of all information which school hold about their child. What should we do?

A. This is what is known as a "**Subject Access Request**". However, because it refers to a child's educational records, there are specific rules. First of all, does the solicitor's letter include with it a signed statement of authority from either the child (if over 12) or from the parent stating that the information may be released to the solicitors in question? If not, then you must ask the solicitor to provide this; otherwise, you may be disclosing information without consent.

If a statement of authority is enclosed then you may proceed to gather the information ready for disclosure. However, before it is disclosed, make sure that you have absolutely everything from which the child can be identified (including information which might only show the child's UPN but not his or her name – the child can still be identified from this). This should be both paper based and computerised information (including e-mails).

Next, you must remove the names of any other children that might appear on the same records in order to respect their privacy. However, because the request is for an educational record, you should not remove the names of school or LEA staff (this is stated in a specific order relating to education record requests). However, information held from other sources such as a medical report from hospital, which forms part of a statement, must not be disclosed without consent from the organisation (unless you are ***absolutely sure*** that parents have already had a copy). The information should then be disclosed together with an explanation about where the information is from; why it is held; with whom it may have been shared outside of school,(e.g. the DfES or Education Leeds) and including an explanation of any codes used.

If any exemptions have been applied then the reason for this must be explained. Exemptions might include that to disclose the information might prejudice the investigation of crime or the collection of taxes or that the disclosure might cause damage or distress.

School can choose to charge up to £50 depending on the number of sheets disclosed (e.g. 100 sheets = £10, 200 sheets = £20 etc). It is sensible to have a standard and published charging policy, which can be made available upon receipt of a request. It should also be noted that if school opt to charge for such requests then the first day of the legally required time-scale for response does not commence until payment has been received.

Be especially careful dealing with such requests where the parents are separated or divorced, as one parent is not entitled to see anything about the other.

This is a very basic outline, there may be other considerations not mentioned in this example. Subject access is a complex area and Information Policy can deal with this on your behalf using their training and expertise. If you wish to pass such matters to Information Policy then please provide details as quickly as possible, as there are only 15 school days from school's receipt of the request in which to respond to educational requests.

Personnel

Q. A teacher has applied for a mortgage and school have received a written request asking for employment details including salary. Can these be provided?

A. Have you received a signed statement of authority from the teacher in question allowing this disclosure to be made? If so, then yes. Otherwise, ask the teacher to write a signed note stating that the requested information can be provided.

Q. A teacher has submitted a subject access request, wishing to see all information we hold about her. What should I do?

A. This is an ordinary subject access request, which is not the same as a request for an educational record as in the earlier example. There are forty consecutive days to provide this information and you can only charge £10 maximum. As before, it is a good idea to have a standard and published charging policy to indicate whether or not a charge will be levied. Similarly, should school wish to charge for this then the first day of the legally required response rate does not commence until payment has been received.

First of all, gather ***all*** information from which the teacher can be identified including both paper and computerised records (including e-mail). Next, remove all references to other people where they can be identified unless you can get consent from them to release this information. This might include comments from which someone can be identified, such as a witness statement or complaint. Any information contained in

correspondence from other organisations should not be released without consent from them first. This includes, for example, all correspondence from Education Leeds.

The information should then be disclosed together with an explanation about where the information is from; why it is held; with whom it may have been shared outside of school,(e.g. the DfES or Education Leeds) and including an explanation of any codes used.

If any exemptions have been applied then the reason for this must be explained. Exemptions might include that to disclose the information might prejudice the investigation of crime or the collection of taxes or that the disclosure might cause damage or distress.

Again, this is a very basic outline, there may be other considerations not mentioned in this example. Subject access is a complex area and Information Policy can deal with this on your behalf using their training and expertise. If you wish to pass such matters to Information Policy then please provide details as quickly as possible.

Governors

Q. We'd like to include the address and telephone number of our Governors in our annual school report to parents. Is this acceptable?

A. Not without consent from the governors first. The school governing body may have to take decisions, which some parents may not be happy with. The telephone number could be used to harass or even threaten a governor should the decision be very unpopular. Ask all governors to sign a written declaration if they consent to their name and telephone number being used in this way. If they don't consent then this information cannot be included. If in any doubt, publish school's phone number as a contact point for governors.

Appendix 11

1. Management

Para	Record Series	Retention in School	Action by School
1.1	Minutes and reports of management team meetings	Current year + 3 years	Destroy
1.2	Professional development plans	Current year + 3 years	Destroy
1.3	School development plans	Current year + 3 years	Destroy
1.4	Headteacher's personal filing	Current year + 6 years	Review and transfer selected items to West Yorkshire Archive Service (for permanent preservation or further review as indicated)
1.5	Deputy Headteacher's records	Current year + 6 years	Review and transfer selected items to West Yorkshire Archive Service (for permanent preservation or further review as indicated)

2. Governing Bodies

Para	Record Series	Retention in School	Action by School
2.1	Instruments and articles of government		
	a) Grant maintained schools	Current	Transfer to West Yorkshire Archive Service
	b) Other schools	Current	Destroy (West Yorkshire Archive Service will preserve Education Leeds copy)
2.2	Proceedings: minutes	Current + 6 years	Transfer to West Yorkshire Archive Service
2.3	Proceedings: agenda papers and reports		
	a) Papers from the DFES	Current	Destroy
	b) Papers from Education Leeds	Current	Destroy
	c) Papers from the school staff	Current + 6 years	Destroy
	d) Agenda files	Current	Destroy unless they contain significant material not duplicated in 2.2 or 2.3(c)
2.4	Proceedings of the annual parents' meeting	Current + 3 years	Destroy
2.5	Action Plans	Current + 3 years	Destroy

2. Governing Bodies cont.

Para	Record Series	Retention in School	Action by School
2.6	Statements under the Education Act	Current	Destroy
2.7	Other policy statements	Current	Destroy
2.8	Records of complaints relating to the curriculum	Current + 6 years	Destroy
2.9	Governor training manual	Current	Destroy
2.10	Correspondence files	Current + 6 years	Review and transfer selected items to West Yorkshire Archive Service (for permanent preservation or further review as indicated)
2.11	Proposals for schools to become, or be established as, grant maintained schools	Current + 3 years	Destroy
2.12	Opt–out ballot papers	6 months	Destroy
2.13	Records relating to endowments and trusts	Current + 6 years	Destroy

3. School Organisation

Para	Record Series	Retention in School	Action by School
3.1	Log books	Current + 6 years	Transfer to West Yorkshire Archive Service
3.2	School prospectus	Current + 1 year	Transfer to West Yorkshire Archive Service
3.3	Headteacher's official diary	Current + 1 year	Destroy
3.4	Staff meeting minutes	Current + 6 years	Destroy
3.5	Administrative and general files	Current + 10 years	Review and transfer selected items to West Yorkshire Archive Service (for permanent preservation or further review as indicated)
3.6	Annual calendar of events	Current	Transfer to West Yorkshire Archive Service
3.7	Circulars to staff	Current + 2 years	Transfer to West Yorkshire Archive Service
3.8	Circulars to pupils	Current + 2 years	Transfer to West Yorkshire Archive Service
3.9	Newsletters to parents	Current + 3 years	Transfer to West Yorkshire Archive Service
3.10	Staff handbook	Current	Transfer to West Yorkshire Archive Service
3.11	Visitors book	Current + 5 years	Transfer to West Yorkshire Archive Service

4. School Council

Para	Record Series	Retention in School	Action by School
4.1	Secretary: Minute books	Current + 3 years	Transfer to West Yorkshire Archive Service
4.2	Secretary: correspondence and notices	Current + 3 years	Transfer to West Yorkshire Archive Service

5. Liaison with the Local Education Authority, Department for Education and Employment, and the Funding Agency for Schools

Para	Record Series	Retention in School	Action by School
5.1	Circulars	Current	Destroy (West Yorkshire Archive Service will retain central set)
5.2	Education bulletin	Current + 2 years	Destroy (West Yorkshire Archive Service will retain central set)
5.3	DfES Returns: PLASC	Current + 6 years	Transfer to West Yorkshire Archive Service
5.4	DfES Returns: records of extra-district pupils	Current + 6 years	Destroy
5.5	September organisation forms	Current + 1 year	Destroy
5.6	Attendance returns	Current + 1 year	Destroy
5.7	Secondary transfer sheets	Current + 1 year	Destroy
5.8	Return of traveller children	Current + 6 years	Destroy

6. Inspection

Para	Record Series	Retention in School	Action by School
6.1	HMI Reports	Current + 6 years	Destroy
6.2	Education Leeds advisory/inspection Reports	Current + 6 years	Destroy
6.3	Independent inspector's reports	Current + 6 years	Destroy
6.4	Papers for inspection	Current + 6 years	Destroy

7. Health and Safety

Para	Record Series	Retention in School	Action by School
7.1	Health and Safety policy statement	Current + 1 year	Destroy
7.2	Accident Books	Current + 3 years	Destroy
7.3	Safety incident report books	Current + 20 years	Destroy
7.4	COSHH (Control of Substances Hazardous to Health) assessment recording book	Current + 5 years	Destroy
7.5	COSHH control measures record	Current + 5 years	Destroy
7.6	Health surveillance records	Current + 30 years	Destroy
7.7	Record of reportable injuries and dangerous occurrences	Current + 10 years	Destroy
7.8	Record of reportable diseases	Current + 10 years	Destroy
7.9	Risk assessments	Current + 10 years	Destroy
7.10	Risk control measures records	Current + 10 years	Destroy
7.11	Maintenance log book	Current + 10 years	Destroy

7. Health and Safety cont.

Para	Record Series	Retention in School	Action by School
7.12	Records of Personal Protection Equipment (PPE)	Current + 10 years	Destroy
7.13	Training records	Current + 10 years	Destroy
7.14	Health and Safety reports	Current + 6 years	Destroy
7.15	Fire precautions log book	Current + 6 years	Destroy

8. Pupils

Para	Record Series	Retention in School	Action by School
8.1	Admissions registers	Whilst still in use	Transfer to West Yorkshire Archive Service
8.2	Attendance registers	Current + 3 years	Destroy
8.3	Pupil record cards a) Record cards – primary b) Record cards – secondary	 Current Current + 6 years	 Transfer to secondary school Transfer to West Yorkshire Archive Service
8.4	Pupil's educational record	Current + 6 years from date of leaving secondary school	Transfer to West Yorkshire Archive Service
8.5	Pupil files	Current + 6 years	keep a sample of data (e.g. relating to 10 pupils representing a cross section of ability).
8.6	STAR pupil database	Whilst still in use	Keep a sample of data (e.g. a minimum of 10 pupils)
8.7	Punishment books	Whilst still in use	Transfer to West Yorkshire Archive Service
8.8	Absence books	Current + 6 years	Destroy
8.9	Absence letters	Current + 2 years	Destroy

9. Staff

Para	Record Series	Retention in School	Action by School
9.1	Teachers files	Current + 12 years	Preserve a sample to send to archive (e.g. in relation to duties, review, classes taught etc.)
9.2	Salary cards	Current + 85 years	Destroy
9.3	Administrative and technical staff files	Current + 12 years	Keep a sample of data (e.g. e.g. in relation to duties, review etc.
9.4	Statutory sick pay notification	Current + 6 years	Destroy
9.5	Personnel Database	Whilst still active	keep a sample of data (e.g. a basic data set relating to name, address and duties)

10. Teaching and the Curriculum

Para	Record Series	Retention in School	Action by School
10.1	Annual curriculum return a) GM schools b) LEA schools (voluntary, aided and community schools)	 Current + 3 years Current + 3 years	 Transfer to West Yorkshire Archive Service Destroy (Education Leeds set will be retained)
10.2	Interim and final reports of the National Curriculum Council	Current	Destroy
10.3	Curriculum development minutes	Current + 6 years	Transfer to West Yorkshire Archive Service
10.4	Curriculum development files	Current + 6 years	Transfer to West Yorkshire Archive Service
10.5	School syllabus	Current	Transfer to West Yorkshire Archive Service
10.6	Schemes of work	Current	Transfer to West Yorkshire Archive Service
10.7	Timetable	Current	Keep a sample of data (e.g. basic information about the subjects taught, at what time of day and by whom).
10.8	Class record books	Current	Keep a sample of data (e.g. random samples across all classes).
10.9	Mark books	Current	Destroy
10.10	Record of homework set	Current	Destroy

10. Teaching and the Curriculum cont.

Para	Record Series	Retention in School	Action by School
10.11	Teaching aids (commercial)	Current	Keep a sample to send to West Yorkshire Archive Service if permitted by supplier contract
10.12	Teaching aids (home-made)	Current	Keep a sample to send to West Yorkshire Archive Service if permitted by supplier contract
10.13	Pupils work	Current	Keep a sample to send to West Yorkshire Archive Service if permitted by supplier contract
10.14	Examination results – pupil level	Current + 6 years	Transfer to West Yorkshire Archive Service
10.15	Aggregated assessment results		
	a) LEA schools	Current + 5 years	Transfer to West Yorkshire Archive Service
	b) GM Schools	Current + 5 years	Transfer to West Yorkshire Archive Service

11. Finance

Para	Record Series	Retention in School	Action by School
11.1	Annual budget	Current + 6 years	Transfer to West Yorkshire Archive Service
11.2	Budget files	Current + 6 years	Destroy
11.3	Headteacher's budget reports	Current + 1 year	Should be among the governors' records. If not then send to West Yorkshire Archive Service
11.4	Annual statement of account	Current + 6 years	Destroy
11.5	Order books and requisitions	Current + 6 years	Destroy
11.6	Delivery documentation	Current + 6 years	Destroy
11.7	Invoices	Current + 6 years	Destroy
11.8	Bank account records	Current + 6 years	Destroy
11.9	Cashbooks	Current + 6 years	Destroy
11.10	Cash till roll	Current + 6 years	Destroy

11. Finance cont.

Para	Record Series	Retention in School	Action by School
11.11	Dinner registers, records and free meals records	Current + 6 years	Destroy
11.12	Debtors records	Current + 6 years	Destroy
11.13	Budget monitoring tabulations	Current + 6 years	Destroy

12. Property

Para	Record Series	Retention in School	Action by School
12.1	Legal agreements, leases maintenance contracts	Current + 6 years	Destroy
12.2	Register of contracts	Current + 6 years	Transfer to West Yorkshire Archive Service
12.3	Register of tenders and quotations	Current + 6 years	Destroy
12.4	Orders for repairs	Current + 6 years	Destroy
12.5	Records of lettings of school premises	Current + 6 years	Destroy
12.6	Records of insurance (policies and schedules)	Current	Destroy
12.7	Burglary, theft and vandalism report forms	Current + 6 years	Destroy
12.8	Title Deeds	Current	Must be retained
12.9	Maintenance log books	Current + 6 years	Destroy
12.10	Contractors reports	Current + 6 years	Destroy

12. Property cont

Para	Record Series	Retention in School	Action by School
12.11	Inventories of furniture and equipment	Current	Destroy
12.12	Registers of loans	Current + 12 years	Destroy
12.13	Capital grant and loan sanction file	Current + 12 years	Destroy
12.14	Plans (e.g. CAD and blue-prints)	Whilst Active	Transfer to Archive

13. Careers

Para	Record Series	Retention in School	Action by School
13.1	Correspondence files	Current + 6 years	Transfer to West Yorkshire Archive Service
13.2	Information files	Current	Destroy
13.3	Service level agreements	Current	Transfer to Careers Service

14. Extra Curricular and Miscellaneous Activities

Para	Record Series	Retention in School	Action by School
14.1	School magazines	Preserve permanently	Transfer to West Yorkshire Archive Service
14.2	Scrapbooks	Current + 1 year	Transfer to West Yorkshire Archive Service
14.3	Photographs	Current	Transfer to West Yorkshire Archive Service
14.4	Programmes	Current + 1 year	Transfer to West Yorkshire Archive Service
14.5	School History (such as honour roles)	Preserve permanently	Transfer to West Yorkshire Archive Service
14.6	Audio – recordings in any format	Current	Transfer to West Yorkshire Archive Service
14.7	Video – recordings in any format	Current	Transfer to West Yorkshire Archive Service
14.8	Annual speech day reports and prize lists	Current + 6 years	Transfer to West Yorkshire Archive Service
14.9	Records of school societies	Current	Review and liase with West Yorkshire Archive Service

15. Old Pupils Associations

Para	Record Series	Retention in School	Action by School
15.1	Secretary: minute books	Current + 6 years	Transfer to West Yorkshire Archive Service
15.2	Secretary: correspondence	Current + 6 years	Review and transfer to West Yorkshire Archive Service
15.3	Secretary: publications	Current + 6 years	Transfer to West Yorkshire Archive Service
15.4	Secretary/Treasurer: membership list	Current	Retention decisions depend upon the form in which the records are kept
15.5	Treasurer: annual accounts	Current + 6 years	Transfer to West Yorkshire Archive Service
15.6	Treasurer: account book (or digital equivalent)	Current + 6 years	Retention will depend upon historical value of information
15.7	Treasurer: other accounts	Current + 6 years	Destroy

16. Parent – Teacher Associations

Para	Record Series	Retention in School	Action by School
16.1	Minutes	Current + 6 years	Transfer to West Yorkshire Archive Service
16.2	Account Book	Current	Retention will depend upon quality and detail. WYAS can advise you about this.
16.3	Annual statements of accounts	Current + 6 years	Transfer to West Yorkshire Archive Service
16.4	Supporting financial documents	Current + 6 years	Destroy
16.5	Files	Current + 6 years	Review and transfer to West Yorkshire Archive Service
16.6	Newsletters	Current + 6 years	Transfer to West Yorkshire Archive Service
16.7	Audio recordings in any format	Current	Transfer to West Yorkshire Archive Service
16.8	Video recordings in any format	Current	Transfer to West Yorkshire Archive Service
16.9	Photographs in any format	Current	Transfer to West Yorkshire Archive Service

Appendix 12

Sample Declarations for School Forms

The wording of the appropriate declaration (or Fair Processing Statement) for your form is dependent on a number of factors. These include the following:

- Whether or not you are asking for information in connection with a statutory duty (for example, Health and Safety legislation);
- Whether or not you are asking for any sensitive personal information (for example ethnicity, matters of health, religious belief etc.);
- Whether or not you might further disclose the information gathered to another organisation.

An indication of the kind of purpose for which the following examples might be used is provided with each sample declaration.

1. Declaration for a form containing sensitive personal data with no overriding statutory authority. This type of declaration might be used for a school trip form where information about a child is needed in order to provide for their special needs.

Data Protection Act 1998

We have an obligation under the Data Protection Act to inform you of the following. By signing this form you are giving your explicit consent to Sometown Primary School processing the information you provide. The processing involved will be for the purposes of organising the proposed school trip. This information may be passed to the coach company and also to the hotel where we will be staying but this will only occur where it is absolutely necessary. We may also use the information you provide for monitoring and statistical research purposes although you will not be identifiable from this. You can contact the school Secretary for further information.

Declaration

I consent to Sometown Primary School processing the information detailed in this form. I understand that this will be used by school only in pursuance of legitimate business purposes and my consent is conditional upon Sometown Primary School complying with their obligations under the Data Protection Act 1998.

Signature _____ **Date** _____

2. This is an example of a voluntary declaration (i.e. non-statutory). In this example (travel claims), no sensitive personal information is being collected and therefore, no signature is required. The completion of the form itself is actual consent to the processing involved. This could be used in school for any form where no sensitive personal information is being requested, for example, attendance at a school play.

Data Protection Act 1998

Under the terms of the Data Protection Act 1998 we must inform you of the following. Completion of this form is voluntary; therefore by doing so you are giving your explicit consent to Sometown Primary School to process your data. The processing involved will be for the purpose of administering your claim for expenses. We may also use the information you provide for monitoring and statistical research purposes. Your information will be shared with Education Leeds who provide this service on our behalf and with Leeds City Council's IT Services Agency who maintains the computer system onto which it is entered. This information will only be used by Sometown Primary School in pursuance of its business purposes and your consent is conditional upon Sometown Primary School complying with their obligations under the Data Protection Act 1998.

3. This is an example of a declaration used on a form collecting information under a statutory duty. Even if this contains sensitive personal information, no signature is necessary because of the statutory obligation to complete the form. School could use such a declaration on any form where a statutory authority (the relevant parts of which must be quoted) is being exercised.

Data Protection Act 1998

Under the terms of the Data Protection Act 1998 we must inform you of the following. By completing this form you are giving your explicit consent to Sometown Primary School processing your data. The processing involved will be for the purpose of administering your application to become an authorised minibus driver in connection with Section 19 Permit requirements of the Transport Act 1985. We may also use the information you provide for monitoring and statistical research purposes although you will not be identifiable from this. The information you provide to us may be shared with other Leeds schools, Education Leeds and Leeds City Council services.

Sometown Primary School will only use your information in pursuance of our business purposes and your consent is conditional upon us complying with our obligations under the Data Protection Act 1998.

4. This is an example of a school form where an additional statement is included to inform parents that children should be given a choice about whether or not to consent to processing of their information once they are old enough to understand the implications.

Data Protection Act 1998

For pupils approaching or above age 13, schools are required to pass on information to the Connexions Service. This information includes the name and address of the pupil and parent(s), and any further information relevant to the Connexions Service's role, which is to support young people, helping them to achieve their potential and to realise benefits from education, learning and employment. In Leeds, this information is passed to Connexions via Education Leeds. However, parents or the pupils themselves if aged 12 or over can ask that no information beyond name and address *(for pupil and parents)* be passed on to Connexions. If as a parent, or as a pupil aged 12 or over, you do not want Connexions to receive information beyond name and address, then please contact school as soon as possible after receiving this note. Since the right to ask for information beyond name and address not to be passed to Connexions rests with pupils if 12 or over, *(rather than parents)*, it is particularly important that you share this note with your child if they are of this age. (DfES) and to the Qualifications and Curriculum Authority (QCA) which is responsible for the National Curriculum and associated assessment arrangements. There is also a new requirement for schools to pass information about pupils who are approaching or are above age 13 to the Connexions Service.

Appendix 13

Data Protection Act 1998
School Subject Access Request Form

The Data Subject **is the person whose personal data are held by school.**

1. Details of the person wishing to access their personal information from school (the *Data Subject*).

Full Name: _____ Date of Birth: _____

Current Address _____

_____

_____

Post Code: _____

Tel No: _____ Email: _____

2. Have you lived in a different address in the last 2 years? If you have, please give the addresses you have lived in previously. (This is to help school locate your personal data.) If you have not, please go to section 3.

Previous Address 1

_____

_____

_____

Previous Address 2

_____

_____

_____

3. Are you the person named in 1 above? Yes ☐ No ☐ (tick one box)
(The *Data Subject*)

If "Yes", Please provide evidence of your identity.

Driving Licence
Pension Book
UB40
Council Tax bill
Other evidence

Please answer question 5 next.

If "No" you *must* provide *written* evidence that you have the Data Subject's authority to ask for the information on their behalf, e.g. a letter written by them, evidence of Power of Attorney, etc.

Please answer question 4 next.

4. If you are ***not*** the person about whom school is holding the data, please give your:

Full Name: _____

Current Address: _____

_____

Post Code: _____

Tel No: _____ Email: _____

What is your relationship to the data subject: -

_____

5. Please describe the information you are seeking. For example, are you seeking information about your child's Statement of Special Educational Needs, or about a specific incident involving your child in school or do you wish to see all information held? Please provide any relevant information to help us to locate the information you need.

_____
_____
_____
_____

6. **Declaration** – to be signed by all applicants. Please note any attempt to mislead may result in prosecution.

I …… To the best of my knowledge certify that the information I have given on this form is true. I understand that school needs to be satisfied about my identity. I also understand that school might need to ask me for more details, in order to locate the information I am seeking.

Signed: _____

Date: _____

Note: school must respond to your request within 15 school days if this request is about your child or 40 days if the request is about you yourself. However, this period will not start until school is satisfied about your identity, and has enough detail to locate the information your are seeking.

Please return this completed form to the school office.

For School Use Only.

Evidence of applicant's Identity checked.	☐
Evidence of Data Subject's Identity checked (if different)	☐
Photocopy of ID materials taken.	☐
Written authority supplied (if not the Data Subject)	☐

Appendix 14

Sometown Primary School
Personal Data Handling Policy

Introduction

This is a statement of personal data handling policy in compliance with the Data Protection Act 1998 as adopted by the Headteacher and Governors of our school. All staff involved with the collection, processing and disclosure of personal data have been made aware of their duties and responsibilities within this document.

Our school needs to collect and use certain types of information about people with whom it deals in order to operate. These include current, past and prospective employees, suppliers, pupils and school staff, clients and customers and others with whom we communicate. In addition, we may be occasionally required by law to collect and use certain types of information of this kind to comply with the requirements of government departments and agencies, for example, the Department for Education and Skills and the Qualifications and Curriculum Authority.

This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer or recorded on other material and there are safeguards to ensure this in the Data Protection Act 1998.

We recognise that the lawful and correct treatment of personal information by our school is very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. We therefore ensure that our school treats personal information lawfully and correctly.

Data Protection Principles

To demonstrate our commitment, we fully endorse and adhere to the Principles of data protection as set out in the Data Protection Act 1998.

Specifically, the principles require that personal information:

a) Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions set out in the Data Protection Act 1998, are met;

b) 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;

c) Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;

d) Shall be accurate and, where necessary, kept up to date;

e) Shall not be kept for longer than is necessary for that purpose or those purposes and retained only for as long as necessary;

e) Shall be processed in accordance with the rights of data subjects under the Act;

Also that:

g) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, damage or destruction to personal data;

h) Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory is subject to a ***'Community Finding***' by the European Commission, which permits transfer.

Our Commitment

Our school will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality and accuracy of personal information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Ensure that everyone managing and handling personal information is appropriately trained to do so;
- Deal with queries about personal information promptly and courteously.

Disclosure of Personal Information

In general, school will only disclose personal information about individuals with their consent. However, there are circumstances under which personal information may be disclosed without consent. Some of these are listed below:

- In connection with any legal proceedings or for the purposes of the detection and prevention of crime;
- In connection with any statutory, legal duty or instruction from a Government Department to do so, such as in connection with Health and Safety legislation or the submission of the Pupil Level Annual School Census (PLASC).
- In connection with payroll and staff administration, personal information may be disclosed to the Local Education Authority or its agents, (e.g. Education Leeds).

In any event, personal information will only be disclosed with proper justification under the Data Protection Act 1998.

School's Notification Entry

School is properly notified (registered) under the Data Protection Act 1998 so that our processing of personal information is lawful. Our notification entry can be checked on-line at www.dataprotection.gov.uk by accessing the Register of Data Controllers. Alternatively, a copy of our notification entry can be checked by appointment in school.

Further Information

You can exercise your rights or find out more information about our school personal data handling policy from the school office on Leeds (0113) 111111. You can also contact the Information Policy Section at Education Leeds for more information about this area on Leeds (0113) 2477889, 3950780 or in writing to:

Information Policy Section, 10th Floor East, Merrion House, Leeds, LS2 8DT

or by email to educ.info.policy@educationleeds.co.uk.

Important Notice

All school staff have a duty to make sure that they comply with the requirements of the Data Protection Act 1998. In particular, all staff must ensure that records are: -

- ✓ Fair
- ✓ Accurate and where necessary up-to-date
- ✓ Kept and disposed of safely and securely

Individual members of staff can be liable in law under the terms of this Act. They may also be subject to claims for damages from persons harmed or who suffer distress as a result of inaccuracy, unauthorised use or disclosure of their data. Any deliberate breach of this policy will be treated as a disciplinary matter and serious breaches of the Act may lead to dismissal.

This policy was approved by:

Name: _____

Designation: _____

Signature: _____

Date: _____

Appendix 15

Agreement to Conduct Research

1. Introduction

1.1. This Agreement is between [***school name***] and [***name of the researcher and institute***].

1.2. The aim of this Agreement is to ensure that research work using personal data is undertaken in accordance with the terms of the Data Protection Act 1998. While this Act is the primary legislation that will govern this Agreement, the parties also recognise that the Human Rights Act 1998 may impose superior conditions on this Agreement.

1.3. Both parties will at all times have particular regard to the Data Protection Principles contained in Schedule 1 of the Data Protection Act 1998.

2. Definition of the Data Set

2.1. Data will be provided by [***name of school***] exclusively to [***name of the researcher/institute***]. The data may not be distributed in any way to any other individual or organisation without the prior written agreement of [***name of school***]. The data set comprises: -

- [***Exact and precise description of the data set to be inserted here including field names***].

3. Conditions under which the Data Set may be used

3.1. The data contained in the data set will contain personal information that is governed by the Data Protection Act 1998. While the Act allows this data to be used for legitimate research purposes, it is important to understand that the Act also imposes a number of conditions for the use of [***data set summary name***]. These conditions include: -

- The raw data will be kept secure at all times
- No other person(s) other than the research team will be permitted to have any access to the raw data
- The raw data will not be published in any form under any circumstances
- Any example data quoted in any research report will confine itself to general cases and no living individual will be identified in any way directly or indirectly
- When the research project is completed, all copies of the raw data will be permanently destroyed

3.2. The research is wholly the responsibility of [***name of the researcher/institute***] and under no circumstances is it to be represented as the work of [***name of school***]. [***Name of the researcher/institute***] must not seek to use [***name of school***] name to suggest any approval nor to seek to encourage data subjects to participate in it.

3.3. Should the research result in publication of findings then neither the school name nor that of the Local Education Authority (or its representatives) may be quoted unless agreed beforehand in writing with the Head Teacher.

4. Summary of Research

4.1. The [***name of the researcher/institute***] agrees to provide [***name of school***] with a

summary of the research findings. These findings may be used by [***name of school***] to improve its services in any way it considers necessary. Any such action by [***name of school***] will not incur any charge or liability towards [***name of the researcher/institute***] or vice versa.

5. The Agreement

5.1. It is a cardinal condition of this agreement that the privacy of the individuals and the confidentiality of the information contained in [***data set summary name***] is always maintained.

5.2. Any failure to meet this cardinal condition and the conditions in Section 3 above may breach the Data Protection Act 1998. Should there be any evidence that this may have occurred, [***name of school***] will consider this to be a fundamental breach of this Agreement and will suspend any cooperation with [***name of the researcher/institute***]. Further, any suspected breach may be reported for investigation by the Information Commissioner or the Courts.

For [*name of school*]	**For [*name of the researcher/institute*]**
Signed: ……..	Signed: ……..
Name: ……..	Name: ……
Position: ……	Position: ……..
School: …….	Institute: ……
Date: ……	Date: ……

Index