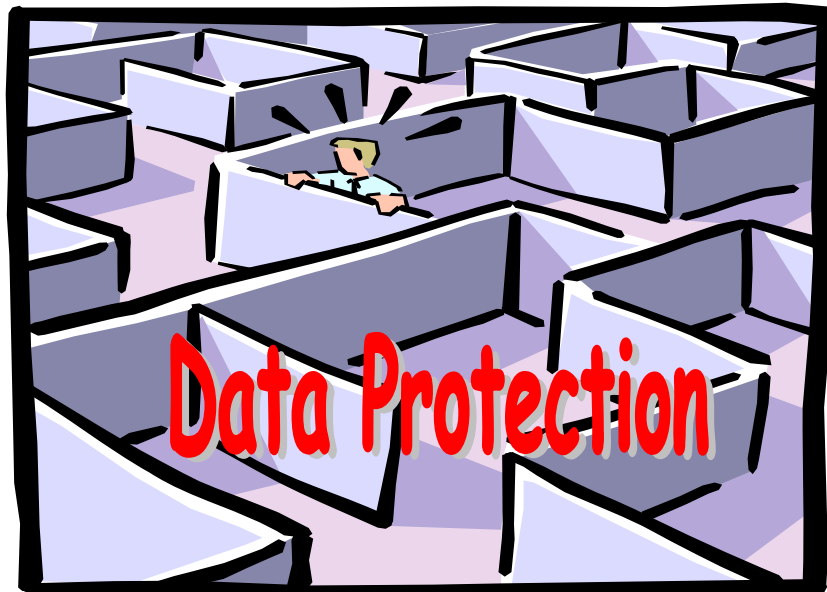




**SOUTH EASTERN EDUCATION
AND LIBRARY BOARD**

Data Protection Schools Guidance Handbook 2007



Please note: This document is intended to act as a general guide for school staff to follow when dealing with personal information during their daily work. The topic is very complicated so it should not be taken as an absolute statement of the law and obligations covered by the Data Protection Act 1998. It is a criminal offence to break any conditions of the Act, so you should always follow your schools procedures on handling and releasing information. The Information Commissioner operates a Data Protection Help Line at Telephone 01625 545 745 or e-mail to <mailto:mail@ico.gsi.gov.uk>

Contents

| | |
|--|-------------|
| Introduction | Page 3 |
| 1. What is the Data Protection Act? | Pages 3-4 |
| 2. Definitions | Pages 4-6 |
| 3. Data Protection Principles | Pages 6-14 |
| 4. Content of Forms/Data Protection Statements | Pages 14-16 |
| 5. The Internet | Pages 16-17 |
| 6. Marketing | Pages 17-18 |
| 7. Home Working | Pages 18-19 |
| 8. Day-to-Day Working | Pages 19-20 |
| 9. Disclosures | Pages 21-24 |
| 10. Data Subjects' Rights | Pages 24-25 |
| 11. Dealing with a Data Subject Notice | Pages 25-26 |
| 12. Receiving a Subject Access Request | Pages 26-28 |
| 13. Training- Who Needs What? | Pages 28-29 |
| 14. Frequently Asked Questions | Pages 29-32 |
| 15. Examples of Disclosures! | Pages 32-33 |
| 16. Notification? | Pages 33-34 |
| 17. Specimen Form 81- PSNI | Pages 35-36 |
| 18. Further Guidance/Contact Details | Page 37 |

Introduction

This practical everyday guidance is offered to Head Teachers, Governors and all school staff who may come into contact with personal data during the course of their duties, in view of questions that are often asked and of situations that have arisen within schools.

In legal terms, schools are classed as separate entities for data protection purposes, known as "Data Controllers", rather than as a collective part of the board. However, the board feels it appropriate to offer advice where requested, in order to maintain a uniformity of practice across schools in the boards administrative area.

1. What is the 1998 Data Protection Act?

The 1998 Act, which came into force on 1 March 2000, replaces the 1984 Data Protection Act, which regulated the use of automated data only. Although there was a changeover period between the old and new acts, we have had to be fully compliant with the terms of the 1998 Act since 23 September 2001.

The 1998 Data Protection Act is concerned with 'personal data'. This data relates to identifiable living individuals. It can be as simple as a name and address. The Act sets out rules for processing personal information and applies to recorded information, whether stored electronically on computer or in paper based filing systems.

The Act works in two ways. It gives individuals certain rights (which have been enhanced under the 1998 Act), whilst ensuring those who record and use the individual's information abide by certain rules. These rules are known as the Data Protection Principles.

The Data Controller decides how and why personal data is processed. Each school and its employees must comply with the data protection principles and other requirements of the Act.

Please note it now states in the Act that:

"Individual officers can be liable where it can be shown they acted outside their authorised limits or if they deliberately or recklessly acted in breach of the law"

Schools must register with the Information Commissioner; this is referred to as NOTIFICATION. A guide on how to complete notification is available on the Information Commissioners Website at:

<http://www.ico.gov.uk/> or the notification help line at

telephone 01625 545 740. or <mailto:data@notification.demon.co.uk>

Please refer to page 34 for further details.

2. Definitions



A number of terms are defined here as they are used frequently when discussing data protection issues.

Data is information that:

- is processed automatically;
- is recorded with the intention that it should be processed automatically;
- is structured as part of a relevant filing system in such a way that information relating to an individual (either by reference to the individual or by criteria relating to an individual) is **readily** accessible; (Refer to the Information Commissioners web site for information on the Durant ruling which impacts on definitions of " relevant filing systems " and " personal information" - Dec 2003) <http://www.ico.gov.uk>
- forms part of an accessible record.

Personal data is data that related to a living individual who can be identified. Addresses and telephone numbers are especially vulnerable to abuse, but so are names and photographs if published in the wider environment of the press, internet or media.

Processing has a very wide meaning and covers everything from creating to destruction. For example, recording, operating and storing information.

The **Data Controller** is the person, company or organisation processing personal data, in this case, the school. **Under the 1984 Act, the school and governing body held two separate registrations but, under the 1998 Act, one notification covers the school as a whole.**

The **Data Subject** is the person to whom the information relates. In the case of **most** children, who are unable to understand the principles of data protection, the parent or guardian will represent the data protection interests.

A 14 year old pupil may well be his/her own data subject and head teachers will need to consider this.

A **Data Processor** is any person (other than an employee of the data controller) who processes data on behalf of the data controller.

The **Information Commissioner** is an independent officer appointed by Her Majesty the Queen and who reports directly to parliament. (Previously called the Data Protection Commissioner, before acquiring an additional responsibility for Freedom of Information legislation)

Notification is the process of registering a database containing personal data with the Information Commissioner so it may be used legitimately. **Currently, only computer databases need to be notified.** You can choose to include your manual records, however, this is completely voluntary. For further information about manual records refer to "The Data Protection Act 1998 An Introduction " available at the information commissioner's website,

<http://www.ico.gov.uk/>

A **recipient** is any person to whom data is disclosed (including employees or agents of the data controller, a data processor, or an employee or agent of the data processor) in the course of processing data for the data controller.

An **authorised disclosure** of information is one for which permission has been received from the data subject or is covered by the terms of another data protection principle.

An **unauthorised disclosure** of information is one for which permission has not been received from the data subject and is not covered by the terms of another data protection principle.

3. Data Protection Principles

There are eight data protection principles that set standards, which staff should observe and adhere to when handling personal data.

First Principle- Fair and Lawful Processing

*"Personal data shall be processed fairly and lawfully and in particular shall not be processed unless at least one of the conditions in **Schedule 2 of the Act** are met, and in the case of sensitive personal data at least one of the conditions of **Schedule 3 of the Act** is also met".*

A data subject must be informed of the identity of the data controller, the purpose(s) for which their data is to be processed and any other necessary information.

One of the following six conditions contained in **Schedule 2** must be met before processing can occur:

Condition 1

The data subject has given their consent to the processing.

Condition 2

Processing is necessary for the performance of a contract or for taking steps for entering into a contract with the data subject.

Condition 3

The processing is required under a legal obligation to which the data controller is subject, other than into a contract with the data subject.

Condition 4

The processing is necessary to protect vital interests (matters of life and death) of the data subject.

Condition 5

The processing is necessary:

- a) for the administration of justice;
- b) for the exercise of any functions conferred on any person by or under any enactment;
- c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department;
- d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

Condition 6

The processing is necessary in order to pursue the legitimate interests of the data controller or third parties or parties to whom the data are disclosed unless it could prejudice the rights and freedoms or legitimate interests of the data subject.

In the case of **sensitive personal data**, one of the conditions of **Schedule 3** must also be met in addition to a condition from Schedule 2.

Sensitive personal data includes:

- the racial or ethnic origin of the data subject;
- their political opinions;
- their religious or other beliefs of a similar nature;
- their trade union membership;
- their physical or mental health or condition;
- their sexual life;
- the commission or alleged commission by them of any offence (civil law); or

- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings (criminal law)

The conditions of **Schedule 3** are:

Condition 1

Having the explicit consent of the individual.

Condition 2

Being required by law to process data for employment purposes.

Condition 3

Necessary to process the information in order to protect the vital interests of the data subject or another person. This applies where consent cannot be expected to be reasonably obtained by, or on behalf of the data subject, or
In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Condition 4

(For this condition to apply you must meet all sub paragraphs i.e. a, b, c, and d.)

The processing;

- a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes and which is not established or conducted for profit;
- b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes; and
- d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

Condition 5

The data subject has made the information public.

Condition 6

The processing:

- a) is necessary for the purpose of or in connection with any legal proceedings (including prospective legal proceedings);
- b) is necessary for the purpose of obtaining legal advice or
- c) is otherwise necessary for the purposes of establishing, exercising or defending rights.

Condition 7

The processing is necessary:

- a) for the administration of justice;
- b) for the exercise of any functions conferred on any person by or under an enactment; or
- c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Condition 8

The processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care treatment and the management of healthcare services) and is undertaken by:

- a) a health professional; or
- b) a person who in the circumstances owes a duty of confidentiality, which is equivalent to that which would arise if that person were a health professional.

Condition 9

(For this condition to apply you must meet a, b and c.)

The processing:

- a) is of sensitive personal data consisting of information as to the racial or ethnic origin;
- b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and

c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

Condition 10

The personal data is processed in circumstances specified in an Order made by the Secretary of State.

Second Principle - Specified Purpose.

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes"

This means you cannot use information for a purpose it was not given for. For example, a school should not use its database of pupil's and/or parents and staff to send out mail shots of services offered by local organisations or businesses, however useful. This information was not given for that purpose, just for administration of the child's progress through the education system.

Third Principle - Adequate, Relevant and Not Excessive.

"Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed"

You should not have too little information for a purpose as well as not having too much! You should not be recording information because it 'might be useful in the future'.

Fourth Principle - Accurate

"Personal data shall be accurate and, where necessary, kept up to date"

It is not sufficient to sit back and wait for people to notify you of changes of address or telephone number. Whilst it may be unnecessary to send out individual data checking paperwork, schools should issue regular reminders via newsletters and notice boards or include a reminder in any general correspondence of the need to notify them of any changes, to demonstrate

their ability to comply with this principle. Best practice is that schools issue information to parents annually to check pupil details are accurate. Staff personal data also needs to be kept up-to-date and reminders should be given at least annually.

Fifth Principle - Not kept Longer than Necessary

" Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes"

In general schools are good at keeping information for the minimum periods that are regulated, be it for legal reasons, audit guidance or board request. A common problem, however, is that where there is no 'retention schedule' in place, obsolete information is often kept for longer than is actually necessary.

The introduction of the Freedom of Information Act 2000 means that public authorities (this includes schools) will have to think about:

- What they record;
- How they record it;
- Who they circulate it to; and
- What they keep



For information on retention and disposal of records, schools can access the model Disposal of Records Schedule from the Department of Education Website www.deni.gov.uk.

Sixth Principle- Data Subjects' Rights

"Personal data shall be processed in accordance with the rights of data subjects under this Act."

A person will contravene this principle if they:

- Fail to properly respond to a subject access request.
- Fail to respond to notices from individuals exercising their rights:
 - to prevent processing likely to cause damage or distress

- to prevent processing for direct marketing
- to prevent processing in relation to automatic decision- making.

Seventh Principle- Security

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

Care needs to be taken to safeguard personal data held within the school. This will cover access controls (to buildings, filing cabinets, computer data etc). Schools should ensure that access to personal data is on a need to know basis and staff are fully aware of access rights. When using the services of a data processor, security arrangements must form part of a written agreement between the two parties.

Eighth Principle- Overseas Transfer.

"Personal data should not be transferred to a country or territory outside the European Economic Area (EEA) unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data".

*The EEA consists of the 25 European Union (EU) Member States, which are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy Luxembourg, Netherlands, Portugal, Spain, Sweden and the United Kingdom.

NEW- Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia.

together with Norway, Iceland and Liechtenstein. The only other country currently having recognised legislation is Uruguay. The United States of America has set up a system which is essentially a series of places and organisations who will act as 'receivers' of information, but the country as a whole still does not have legislation up to the standards required by our own, and European Directives. (* at May 2004)

When deciding what amounts to an adequate level of protection the following points should be considered.

- The nature of the personal data;
- The country or territory of origin of the information contained in the data;
- The country or territory of final destination of that information;
- The purpose and period of processing;
- The law in force in the country or territory in question;
- The international obligations of that country or territory;
- Enforceable codes of conduct or other rules enforceable in that country or territory;
- Any security measures taken in respect of the data in that country or territory.

To export personal data outside of the EEA a condition from Schedule 4 of the Act must be met, as well as considering the above points. i.e.

Condition 1

The data subject has given their consent to the transfer.

Condition 2

The transfer is necessary for the performance of a contract between the data subject and the data controller, or with a view of entering into a contract with the data controller.

Condition 3

The transfer is necessary for the conclusion of a contract between the data controller and a third party, which is entered into at the request of the data subject, or is in the interests of the data subject or for the performance of such a contract.

Condition 4

The transfer is necessary for reasons of substantial public interest.

Condition 5

The transfer is necessary for the purpose of, or in connection with, any legal proceedings (including any prospective legal proceedings) is necessary for obtaining legal advice, or is necessary for establishing, exercising or defending legal rights.

Condition 6

The transfer is necessary to protect the vital interests of the data subject.

Condition 7

The transfer is part of the personal data on a public registrar and any person to whom the data are or may be disclosed after the transfer complies with any conditions subject to which the registrar is open to inspection.

Condition 8

The transfer is made on terms of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.

Condition 9

The transfer has been authorised by the commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

4. Content of Forms/Data Protection Statements -

School will collect personal data about pupils, staff etc through the use of forms. The personal information being collected must be justifiable (see Principle No. 3) and that it is clear what the data is to be used for. In this respect forms may need to declare the purpose of collecting/holding/processing the data and offer an assurance as to its processing.

(Sensitive Personal Data)

It is likely that virtually all schools hold data, which is sensitive personal data under the Act. If you collect such data for the purpose of monitoring, i.e. religion or ethnic origin, medical data, you need to satisfy the requirements of Condition 9 of Schedule 3.

The purpose of collecting this type of data should always be stated alongside the question that requests this data. This information should be kept secure and confidential and this should be stated.

If racial and ethnic origin data is being collected for any other reason the purpose must meet another condition within Schedule 3 of the Act before being processed in addition to meeting a condition from Schedule 2.

If in doubt ask yourself the following question:

Is it strictly necessary to know the names of pupils and therefore could this type of data be collected in an anonymous way?

Forms

The following rules should be followed when considering whether a Data Protection Statement is necessary on forms collecting personal data:

- The title on the form should make it obvious to the data subject what their information will be used for. If this is clear a statement as to the purpose is not required.
- Letters and memoranda do not need statements.
- Some forms may be considered as internal data transfer documents and, as such, are not actually used to collect personal data. An example is the petty cash claim form, where the name and address details are already held but are used to identify the claimant against official records.

In order to ensure that processing of personal information is considered to be fair and lawful (meeting the set conditions within Schedule 2 of the Act) it is essential that the school in its role as data controller, ensures that the data subject has been provided with the following:

- That the identity of the data controller is clear; i.e. the name of the school is specified.
- The purpose for which the data is intended to be processed. Quite often, this information may be contained within the title of a form, but if it is not obvious it should be stated.
- Any consequences of such processing which are not obvious to the data subject, and;
- Any anticipated disclosures, which are not obvious to the data subject.

In order to meet bullet points 2-4 as listed above, a data protection statement is often required. This statement must NOT appear in a smaller font than that used for the majority of the form. The statement should ideally appear on the top of the form so that the data subject is made aware of the implications of their data being processed before they start to complete the form.

Suggested Data Protection Statements could be:

(a) If purpose of form is clear from title:

The information on this form is covered by the Data Protection Act 1998.

(b) If purpose of form is unclear:

The information on this form is required for the purpose of <state the purpose>. The information is covered by the provisions of the Data Protection Act 1998. Your signature to the form is deemed to be an authorization by you to allow the School to process and retain the information for the purpose(s) stated.

It may be necessary to inform the data subject how long their data will be kept. This would probably apply whenever the data is kept for longer than the statutory minimum periods and where the information is likely to cause harm or distress if it is used after it becomes inaccurate or out of date.

5. The Internet

When collecting personal information from a data subject using the Internet, always inform the user of:

- who you are, (for example school name and the position held by contact, e.g.: Head Teacher);
- what personal data is being collected, processed and stored;
- the purpose for which the data is being collected;
- the consequences of any processing;
- any envisaged disclosures of personal data.

This is exactly the same, as you would do if you were using a paper form to collect data!

Once you place personal data on the Internet it becomes available worldwide. In many countries the use of personal data is not protected by legislation. It is essential to obtain consent from the data subject before placing their personal data, including photographs, on the Internet.

You should do this before the data subject supplies any information, for example, via an on-line application form.

When compiling information for a web page the following points should be considered if you are intending to collect or hold personal information from a data subject:

- Never collect or retain personal data unless it is strictly necessary for the purpose(s).
- A data subject has the right of rectification, blocking, erasure and destruction of inaccurate data. Any third parties to whom disclosures have been made must be informed of such inaccuracies immediately.
- The data controller must respond to a Data Subject Notice within the prescribed time limits.
- If personal data is required for marketing purposes, a statement should clearly state this and the data subject should be given the option as to whether they wish their details to be used in this way. Ideally, this should be in the form of an "opt in" tick box. However, an "opt out" tick box may be used, thus giving the data subject the opportunity to indicate whether they want their personal data to be processed in this manner.
- If a data subject requests that they do not wish their personal data to be used for marketing purposes then this type of processing must cease immediately.
- If sensitive personal data is being collected, it is **necessary** that a condition from Schedule 3 be also met in addition to a condition from Schedule 3.
- Inform the data subject as to how their personal data will be protected.
- Any anticipated disclosures of personal information, which are not obvious, should be stated along with the reason when collecting the information.
- Personal data cannot be used for any other non- stated purposes.

The board has adopted a policy on use of e-mail and the Internet. It is recommended that schools should adopt a similar approach themselves.

6. Marketing

An organisation may market/advertise information to the data subject as long as the data subject is informed at the point of collecting their information that this is the case.

The data subject must also be informed as to what personal data will be used for marketing purposes, e.g. name and address. The data subject must also be given the opportunity to prevent this type of processing if they so wish. Therefore, a marketing statement is required. Ideally this should contain an "opt in" tick box, however, an "opt out" tick box may also be used, thus giving the data subject the opportunity to indicate whether they want their personal data to be processed in this manner.

The use of negative consent must stand out through using capitals and/or emboldening the words "do not".

The marketing of sensitive personal data may need explicit, which is usually classed as written, consent.

If using "Yes" and "No" tick boxes, a non-response would not give consent - the legislation does not permit a non-response to be assumed as consent.

If a data subject indicates that they do not want their personal details to be processed for the stated marketing/advertising purpose, this must be honoured and the relevant staff informed, to ensure that the data subject's wish is complied with.

It is not acceptable to use software that does not allow a data subject's personal information to be withheld if they have not consented to marketing of their details - if software does not already allow this facility it should be amended to ensure compliance.

7. Home Working

School staff will inevitably undertake work at home and this will often involve the use of ICT equipment that may hold databases containing personal data. Similarly, paper files containing personal data may also be used away from the school environment.

Permission should always be obtained before processing personal data at home and it should be remembered that the definition of "processing" includes "holding" even if the information is not actually used.

Staff should always take reasonable measures to ensure no unauthorised access can be made to the personal data taken home. This is likely to mean that computers are password protected and are not left unattended with personal data accessible.

Staff should take special care in ensuring that paper files are kept secure and locked away (for example, in a locked briefcase) when not in use. This will ensure that individuals, including family members, do not have access to the personal information, thus ensuring protection against potential unauthorised disclosure, accidental loss or destruction.

Employees who choose to undertake work at home in relation to their official duties using their own ICT equipment must understand that they should not hold any database, or carry out any processing, of personal data relating to the school.

Extra care should be taken when transporting files to and from home. Briefcases or files should be transported in a secure manner and not left on a seat, the roof of the car or on the pavement. Really, this has happened!!!

8. Day to Day Working

The following points are intended to act as a guide for staff to follow when using personal information during the working day:

- ✓ Unauthorised staff and other individuals should be prevented from gaining access to personal information.
- ✓ Visitors should be received and supervised at all times within the school premises, especially where information about individuals is stored.
- ✓ All computer systems containing personal data should be password protected; the level of security will depend on the classification of data being held.

- ✓ Staff should have access to personal information on a "need to know" basis.
- ✓ Computer workstations should not be left signed on when not being used.
- ✓ CDs, disks, tapes, printouts and other storage media containing personal data should be locked away when they are not in use.
- ✓ Be careful about what is sent via email and to whom information is sent. Generally personal data should not be sent in an email unless data can be encrypted or files password protected.
- ✓ The same applies to faxes. If it is absolutely necessary to send personal data via fax then check that the intended recipient of a fax containing personal information is aware that it is being sent in order that they can ensure security on delivery.
- ✓ Ensure that paper files are stored in secure locations and accessed on a "need to know" basis only.
- ✓ Do not disclose personal information to anyone other than the data subject unless you have his or her consent, it is a registered disclosure, or it is required by law or permitted by a Data Protection Exemption. **Always ask for proof of identity before making a disclosure.**
- ✓ When processing personal information do not leave it on public display. All paper files containing personal information should be locked away at the end of each day and not left on desks.
- ✓ Computer monitors should be positioned so that personal data cannot be viewed by anyone not authorised to do so.
- ✓ Security arrangements should form part of a written agreement between the data controller and data processor, if processing is carried out by an external source.
- ✓ Subject to relevant retention periods, redundant personal data should be destroyed by shredding if possible, or by use of an appropriate confidential

waste system. If disposable bags are used, they should not be left lying in corridors for collection. CDs, disks, tapes, and other storage media should be either electronically "wiped" or physically destroyed beyond recovery.

9. Disclosures

Personal information can only be disclosed:

1. to the data subject (the person to whom the data relates);
2. with the data subject's consent;
3. if required in life and death situations (Schedule 2 of the Act);
4. if it is not covered by an exemption;
5. if it is to a notified recipient (a registered disclosure). This would be detailed in the Notification of Personal Data form for automated data; or
6. if the disclosure is necessary to carry out the purpose for which the personal data has been obtained fairly and lawfully (note: the data subject should be aware of such disclosures).

If you need to disclose an individual's information to deal with an enquiry one of points 1 - 6 above should apply. If you are at all unsure about making a disclosure, take the individual's telephone number and speak with your line manager.

Disclosing Information to the Data Subject

Before disclosing any personal information you must be satisfied that you are talking to the data subject by asking for proof of identity. If they have no proof of identity or the enquiry is over the telephone, the following procedure should be followed:

- Ask two questions, which you believe only the data subject could answer, i.e. child's birth date, family names etc.

- The data subject must answer at least two questions correctly before you disclose any personal information to them. If you are at all unsure of the individual's identity or your questions were not answered correctly ask more questions.
- If you are still unsure of the data subject's identity, apologise to the person/caller and explain that you cannot give out any personal information because under the terms of the 1998 Data Protection Act you are unsure of their identity. Advise them to write or return with suitable identification if the information is still required.
- If you are satisfied that you are speaking to the data subject and they have answered at least two questions correctly, they can only be supplied with information which relates to themselves in order to deal with their enquiry.

Disclosing Information with the Data Subject's Consent

If an organisation or individual calls and requests information about an individual, the data subject's consent must be gained before any information is disclosed, unless there is a legislative reason for the disclosure. Such consent may have been given at the point of collection of the personal data, if the person or organisation was listed as a possible disclosure to which the data subject agreed by completing the form.

Should the request be by telephone, first check the caller's identity. To do this check the telephone number by contacting Directory Enquiries and then telephone them back, preferably via a switchboard.

If you are at all unsure of the caller's identity you can refuse to disclose information over the telephone and ask the caller to put their request in writing.

Tracing Disclosures

All disclosures should be traceable in order that any errors may be corrected. Systems should be in place to enable the data controller to trace persons or

organisations to whom personal data has been disclosed. These systems should also include:

- The date
- What was disclosed and why
- Who disclosed the data
- Any other necessary and relevant information relating to the disclosure.

A Data Subject is also entitled to this information when making a Subject Access Request.

Disclosure Log

In the case of a disclosure being necessary without the data subject's prior consent; is not a notified disclosure; is not covered by a disclosure exemption, or does not relate to the purpose for processing the data, **permission must be obtained and details of the unforeseen disclosure must be recorded in a Disclosure Log.**

In the event of inaccurate information being disclosed to anyone, the Disclosure Log would enable a correction notice to be sent to all involved and also provides details of where information has been passed on to in order that it can be traced. The easiest way to comply with this is to use a simple form listing relevant details of the disclosure.

The following information should be recorded:

- To whom was the information disclosed.
- What information was disclosed?
- Why was it disclosed?
- What does the recipient intend to do with the information.
- Would it matter if it were not disclosed?
- Date, time and name of member of staff disclosing the information.

Disclosure of Personal Information Covered by an Exemption

There are a number of exemptions from various provisions of the Act relating to disclosures. The following are the most common exemptions whereby personal information may be disclosed:

- To someone acting on the data subject's behalf who has their written consent.
- For the prevention or detection of crime, apprehension or prosecution of offenders and for taxation purposes.
- Required by Statute, rule of court or by order of the court. A court order or proof of the relevant Act of Parliament is needed.
- National security.
- For obtaining legal advice and in legal proceedings where the person making the disclosure is a party or a witness.
- To prevent damage to anyone's health.

10. Data Subjects' Rights

The 1998 Data Protection Act gives data subjects certain rights in relation to personal data held about them by others. These are listed below with a short explanation as to what they mean:

The Right of Subject Access

This allows data subjects to find out what personal data is held which relates to themselves by making a Subject Access Request.

A Data Subject Notice.

The right to prevent processing likely to cause damage or distress. A data subject can write to a data controller asking for processing to stop, or request that they do not begin processing personal data relating to themselves which is likely to

cause substantial unwarranted damage or distress to themselves or anyone else. This is known as a Data Subject Notice.

The Right to Prevent Processing for Direct Marketing.

A data subject can ask a data controller to stop or not to begin processing personal data relating to him/her for direct marketing purposes. This is an absolute right.

The Right to Compensation.

A data subject has the right to take action for compensation if they suffer damage or damage and distress because of any breach of the Act by a data controller. Compensation for distress alone can only be claimed in limited circumstances.

The Right of Rectification, Blocking Erasure and Destruction.

A data subject may apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

Rights in Relation to Automated Decision-Taking.

A data subject can ask a data controller to ensure that no decision that significantly affects them is based solely on processing their personal data by automatic means.

A Request for Assessment.

Any person has the right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

11. Dealing with a Data Subject Notice

A data subject can write to your school as a data controller requiring the school to cease or not to begin processing their personal data, whereby doing so would, or is likely to cause unwarranted substantial damage or substantial distress to them or to another person. However, this right is unavailable if any one of the following conditions for processing can be complied with:

- Consent of the data subject has been obtained;

- Data is necessary for the performance of a contract with the data subject;
- There is a legal obligation;
- To protect vital interests of the data subject.

Should you receive a Data Subject Notice an indicator must be put on the data subject's record to show that a Notice has been served, when it was served and what actions have been taken.

The school, in its role as data controller, then has 21 days to respond, in writing, to the Data Subject Notice, stating that it has complied or intends to comply. If the school does not intend to fully or partially comply with the Data Subject Notice the reasons for this action should be stated.

12. Receiving A Subject Access Request.

A data subject whose details are held by a school, as data controller, has the right to receive a copy of information held about them.

To obtain this information the data subject will need to make a Subject Access Request in writing. They are then entitled to be told whether the school, or someone else acting on it's behalf, is processing their personal data and if so be given a description of:

- The personal data;
- The purpose(s) for which it is being processed;
- To whom the data are or may be disclosed;
- The source of the information;
- Logic behind processing (except in cases of trade secrets)

A charge can be made to individuals making Subject Access Requests, as set down from time to time by the Information Commissioner.

Staff processing personal data should check their notified systems as soon as possible for information relating to the named person. The Data Protection Act requires data controllers to reply to Subject Access Requests as quickly as

possible and in all cases within 40 calendar days, or later if the data subject has not given enough information for a search to be made.

Education Records

There are different arrangements for some educational records that you need to be aware of. The Act sets out specific rights in relation to educational records held *within the state educational system*. Educational records are records that are the official records for which Head Teachers are responsible.

A period of up to **15 school days** are allowed in which to respond to a subject access request (the equivalent period for other types of records is up to **40 working days**)

Examination Results

For examination results the period is **5 months or 40 days** after results are announced, whichever is the earlier.

See frequently asked questions- page 29

The following basic points should be noted when dealing with a request:

- The data subject has the right to see all of their personal information (unless covered by an exemption).
- A copy should be kept on file of all information sent to the data subject. · All codes to be explained.
- Third party details should not be included without written consent of the third party.
- If dealing with a joint application, the parties must only be given their own information and not the partner's unless written permission is received.
- Once all the information has been gathered, ask the data subject if they would like to collect it or have it sent by registered post.
- The data subject should receive all information within 40 calendar days of their request (in the case of examination results a dispensation exists - five months or 40 days after results announced, whichever is the earlier).

Subject Access Exemptions

There is some information that may be exempt from the Subject Access provisions. If this is the case then the data subject has no right to this

information and must be informed, "I do not hold any personal data that I am required to reveal to you".

The Exemptions are as follows:

- National Security
- Prevention of crime and taxation purposes
- Health, Education and Social Work
- Special Purposes (must meet certain criteria)
 - Journalism
 - Artistic purposes
 - Literary purposes
- Judicial appointments and Honours
- Crown employment and Crown or Ministerial appointments
- Management forecasts/management planning
- Negotiations
- Corporate Finance
- Examination scripts
- Legal professional privilege
- Statistical or research data that does not identify an individual
- Confidential references given by the data controller (but not received by the data controller).
- Data incriminating the data controller:
 - An employee need not comply with any request or order if compliance would expose him/her to proceedings for an offence. (Section 7 of the Act). Information disclosed cannot be used in legal proceedings against the school.

13. Training- Who Needs What?

- It is vital that all staff understand their rights and responsibilities. Data Protection legislation is what is known as absolute law. In other words, if you were to be prosecuted for contravening the terms of the 1998 Data Protection Act you could not use ignorance of the law as a defence.
- Heavy fines, to be paid personally by the individual, and jail sentences can also be imposed. The employer is not legally allowed to reimburse the

individual for these fines. This is in addition to any corporate sanctions that could be imposed against the school as data controller.

- It is recommended that all front-line staff, that is those staff that deal directly with people's personal data, should receive Data Protection awareness training. Other staff should also be aware of the law, although this may be achieved by reading these guidelines or by having material included in induction training sessions.

14. Frequently asked questions

Q: A teacher wants a printout of addresses or telephone numbers on a class list- is this ok?

A: Consider why? If the teacher is taking pupils away on an overnight journey, then the information is necessary. The teacher should keep the printout private and return to the school office for shredding immediately after the event. Otherwise, NO- if the teacher needs to know such details, they will be available from the school office.

Q: At Christmas, parents are requesting lists of children in their child's class, to enable them to send cards to the children and avoid anyone missing out. Is this okay?

A: A list of just names is ok as this information will be freely available to the children in the class anyway. An idea would be to allow older children, who can write, time in class to write out their own list.

Q: The school nurse has noticed a medical condition and wishes to speak to the child's parents about treatment. Is this OK?

A: Consider whether the nurse is working in an official capacity for your school? If the answer is "yes" go ahead and record the information in your Disclosure Log. This would also apply to other people working in an official capacity for your school and could include school dentists, doctors, welfare officers, social workers who you know to be involved with the pupil. Always record the disclosures in your log— you will have forgotten it by the following week!

Q: A private dentist is setting up in the area and would like to mail-shot our families - can I give him the addresses?

A: Do you really need to consider it? The answer is NO! - it is not authorised disclosure. There are circumstances like this where you may consider distribution of mail via the pupils.

Q: The school photographer wants to print names on the frame of a group photograph. Is this OK?

A: Consider whether there are any families who would rather not have their children so identified. All parents should give their written permission- this may sound like unnecessary overkill but it is not as drastic as it sounds. The problem of pupil recognition by those with a sinister purpose cannot be understated. You really have to consider what controls you have over materials where the information is printed. Consider the possibility of an estranged parent- **legally denied all access**- recognising their child from a school photograph and abducting her because they have just discovered which school she now attends.

Q: The local newspaper wants to publish a photograph of a school event. Of course, the children want their names in print-can I release them?

Consider what control you have over the distribution of the newspaper? - the answer to this is ABSOLUTELY NONE! You need permission from the parents of the children in the photograph. Please make sure that neither teachers nor children themselves release their names to any reporter, if parental permission has not been obtained. This example applies equally to television reports and video productions.

Q: I want to put pupil names and/or photographs on the Internet, Can I?

A: Remember that all information passed on the internet goes beyond your control and can be accessed worldwide, including in countries without adequate data protection legislation. Digital photographs and scanned images where pupils can be identified are also covered by the 1998 Data Protection Act, so get written parental permission!

Q: The police want information about one of our pupils who has been up to no good. Surely I can release that?

A: Always ensure the police officer provides a Form 81 declaration, signed by a PSNI officer of the rank of inspector or above that proves that you have taken reasonable care to ensure police entitlement to the personal data (see specimen Form 81 pages 35-36). Also, only give the officer what is necessary, not whole files or printouts relating to a pupil.

Q: A parent wants to see information we hold about his or her child. What do I do?

A: The parent should make a formal subject access request or, if you wish to deal with the situation less formally, agree a mutually convenient place and time to show them their child's records. (Education (Pupil Records) Regulations NI 1998 refers)

In the case of educational records, i.e. these are defined as official educational records, held within the state education system, for which the Head Teacher has responsibility; a period of 15 school days is allowed to reply to a subject access request. For examination results, the period is 5 months or 40 days after results are announced, whichever is the earlier.

Q: A parent refuses permission for us to hold the child's information on our computer. What Do I do?

A: Be diplomatic! You have the right to hold information that you need for administering the child's progress through your school and to disclose it within the terms of your notification and the provisions of the Act.

Q: A parent wants to take their child to a school friend's party, but has lost their home address. Can I release the address?

A: NO-you should telephone the party holder and get permission.

Q: A private company has opened an educational Internet website and requires pupil details so that they can be set up to use it. Can I release the details on disk or paper?

A: It is unlikely that you are notified to disclose information to private companies, even though they may be offering an excellent educational service. If such an activity were to form a regular part of your educational programme, then it would be worth considering altering your notification to include it. Otherwise, "NO", get written permission.

Q: I think it's a good idea to put the addresses, telephone numbers and e-mail contact details of our Governors in the School Prospectus. Does that present any problems?

A: It's a good idea but Governors make decisions that may not be universally popular. Perhaps the release of a telephone number and email address may cause problems. If you particularly want to publish such details, ask the person concerned to sign a note agreeing to the publication of their contact details. If they do not agree, they can still be contacted via the school.

Q: A teacher has applied for a mortgage and the building society has requested that I confirm the person's post and salary details. Can I do this?

A: Yes, but ask the teacher to write a note requesting the release.

15. Examples of Disclosures.

■ This incident happened some years ago in a Midlands school. A family admitted a child to the school, which had in its area a number of military houses. One father was a serving soldier who had been on active service in Northern Ireland. As the entire family had received a personal death threat from a terrorist organisation, they had been moved away and the father assigned other duties. Great caution had to be observed by the school as to who could collect the child at home time. Imagine if that child's photograph and name had been released to the press when a school event was being publicised.

■ In 1999 the national press quoted the case of a convicted paedophile, subsequently released from prison. From his prison cell he made secret plans to re-offend. He got hold of copies of his local newspapers and scoured them for pictures of young girls. He noted the names of dancers and youngsters in school pictures, preparing for the time he was released. Detectives believe he

resumed preying on children as soon as he was released. He used telephone books to find addresses of children he had identified in pictures. He then visited addresses, engaging youngsters in conversation outside their homes. With the methodical attention to detail typical of many paedophiles, he used a map book of the town and the surrounding area, marking the homes of children with their initials. During their enquiry, police officers spoke to seventy children aged from six to fifteen years who had contact with him.

📍 Somewhere in the south of England, a police officer in uniform approached a secondary school and asked for the address of a pupil who he named and said he wished to discuss an incident with him. The police officer said he did not wish to speak to the pupil in school as he may be unfairly judged if he was seen to be questioned by the police at school. This seemed reasonable to the school secretary who gave the police officer the pupil's address. Unfortunately, the real reason the officer wanted the address was that this boy has supplied the officer's teenage daughter with drugs. He went round to the boy's house and beat him up, injuring him so severely the boy ended up in hospital. The police officer was jailed for assault and dismissed from his job, but, from the data protection angle, the **school secretary was fined for making an unauthorised disclosure of personal data.**

16. Notification!



(i) What is notification?

The Data Protection Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. Individuals can consult the register to find out what processing of personal data is being carried out by a particular data controller. Notification is the process by which the data controller's details are added to the register.

(ii) Why do I need to notify?

The Data Protection Act 1998 requires every data controller who is processing personal data to notify. Failure to notify is a criminal offence.

(iii) How do I notify?

There are two easy ways to notify.

(a) By Internet- you can complete the notification form on-line, print it and send the form to the information commissioner with the notification fee (£35- nil vat) or direct debit instructions to <mailto:data@notification.demon.co.uk>

(b) By Telephone- you can telephone the notification help line (01625 545 740)

(iv) How long does my notification last?

The notification lasts for one year and needs to be renewed annually. The office of the information commissioner should write to you before the expiry date of your register entry. The notification fee is an annual charge!

18. Further Guidance/Contact Details.

Remember the importance of observing the terms of the 1998 Data Protection Act as failure to do so may result in prosecution of both individuals and organisations. Ensure all staff are provided with basic awareness training and, at the very least, are given access to these guidance notes.

The Information Commissioner is available to give **specific** guidance on the Act and their website offers readily accessible guidance on all aspects of data protection.

<http://www.ico.gov.uk/>

For **general** advice and/or information, please contact:-

| | |
|--|----------------------|
| Patricia O'Connor (Data Protection Officer) | 028 9056 6275 |
| or | |
| Derek Cunningham (Records Management Officer) | 028 9056 6994 |
| Office of Information Commissioner (Belfast Office) | 028 9051 1270 |
| Office of Information Commissioner (UK) | 01625 545 745 |