

Staff Guide to The Data Protection Act 1998



**SOUTH EASTERN EDUCATION
AND LIBRARY BOARD**

- **This document is intended as a general introduction to the Data Protection Act 1998. However, the topic of this document 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 Unit's procedures on handling and releasing information.**
- **You should ask your line manager for advice if you are unsure about any specific or particular situation presented.**

Contents

	Page
The Data Protection Act 1998	3
Definitions	4
Eight Principles	6
Data Collection – Use of Forms	12
Disclosures	13
Dealing with Subject Access Requests	16
Notification - What Is It ?	18
Security of Personal Information	19
Training – who needs what?	21
FAQ	22
Examples of Disclosures	24
Further Guidance / Contact Information	25
Sample PSNI Form 81	26

The Data Protection Act 1998

What is the Data Protection Act 1998?

It is a law that protects personal privacy and upholds individuals' rights.

Does the Act affect you?

Yes. The Data Protection Act applies to anyone who handles or has access to information about individuals. The Act also gives rights to the people the information is about. By law, everyone in the workplace must follow the rules set out in the Act and help protect individuals' rights.

What are your responsibilities?

The Act helps make sure that the information held on computers and in some paper based systems is managed properly. You must protect personal information by following the eight principles of good practice. (See page 3)

Why do you need to know about the Data Protection Act (DPA) ?

Anyone who handles personal information as part of his or her job must be aware of the DPA. The Act applies to both **employers** and **employees** of the Board.

Definitions

To understand the principles of the Act, you need to know what the main terms mean. Here are some definitions.

Data Controllers: are people or organisations that hold and use personal information. They decide how and why the information is used. As data controllers, employers have a responsibility to establish workplace practices and policies that comply with the DPA.

Data Subjects: are the people the information is about. Within the workplace, they may be current employees, people applying for jobs or former employees. Data subjects might also be pupils, suppliers or other people information is held about.

Data Users: include employees whose work involves processing personal information. As a data user, you have a legal duty to protect the privacy of individuals in the way you handle their information. You must follow your Unit's procedures on handling and releasing information.

Data Processors: may be separate organisations that process information on behalf of data controllers. They must also follow the DPA and make sure information is handled properly and securely.

Data: is recorded information, whether stored electronically on computer or in paper-based filing systems.

Personal: means that the information is about an identifiable *living* being. Personal data can be factual, such as a name, address or date of birth, or it can be an opinion, such as how a manager thinks an employee has performed at an appraisal. It can even include a simple e-mail address.

Definitions (cont'd)

Processing: is any activity that involves the data. This includes collecting, recording or retrieving the data, or doing work on the data, such as organising, adapting, changing, erasing or destroying it.

Sensitive Personal Data: includes information about someone's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexuality, or criminal proceedings or convictions. Sensitive personal data can only be processed under strict conditions. In most cases, this means getting permission from the person the information is about.

The Eight Principles

The Act is based on eight data protection principles, or rules of good information handling.

In summary, the data must be:

1. Processed fairly and legally.
2. Processed for limited purposes and in an appropriate way.
3. Relevant and sufficient for the purpose.
4. Accurate.
5. Kept for as long as is necessary and no longer.
6. Processed in line with the individuals' rights.
7. Secure.
8. Only transferred to other countries that have suitable data protection controls.

The following pages explain these principles in more detail.

First Principle

- **Personal data must be processed fairly and legally.**

Processing applies to all uses of data

From collecting and storing data, to retrieving, organising and destroying it
There are two main conditions to this first principle. Either the data subject must give their permission or the processing is necessary for legal or contractual reasons.

For data to be processed 'fairly':

- the data subject should know who the data controller is;
- why the data is being processed and any other necessary information, such as the likely consequences of the processing.
- individuals must not be deceived or misled as to why the information is needed.

For data to be processed 'legally':

- It must not lead to any kind of discrimination and should not go against other laws such as the Human Rights Act 1998

Second Principle

- **Personal data must only be obtained for specific and legal purposes, and must only be processed in a way that is consistent with the specified purpose.**

Data controllers and data users must not collect and use data unless there is a specific and valid reason for doing so.

The data subject must be told what the information will be used for.

Personal data collected for one reason must not be used for any other unrelated purpose.

For example, names and addresses of staff that are held for employment purposes must not be given to a mail-order company, without their permission. See section on Forms page 10.

Third Principle

- **Personal data must be adequate, relevant and not excessive for the purpose it is processed for.**

Only data needed for the specific purpose should be asked for or recorded. Information that is not relevant for the purpose must not be collected simply because it might be useful in the future!

Likewise, when filling in forms about staff, parents, pupils or other data subjects, you should only record relevant information, not inappropriate personal remarks. These comments would have to be disclosed if somebody asks to see their personal information. (See subject access rights on page 8)

Fourth Principle

- **Personal data must be accurate and where necessary, kept up to date.**

Incorrect and misleading data are inaccurate. Data users should record data accurately and take reasonable steps to check the accuracy of information they receive from data subjects or anybody else.

Managers should review personal information held so that only up to date and accurate information is kept.

Fifth Principle

- **Personal data processed for any purpose must not be kept for longer than is necessary to fulfil that purpose.**

Organisations will need to keep some data on current and past employees to respond to enquiries from a new employer or from the Inland Revenue. Data also needs to be kept to meet legal obligations or to support the business process.

Other types of personal data may not be relevant for future purposes and should not be kept for longer than necessary.

The Board has a **Disposal of Records Schedule** which identifies the retention period of files, including those files which contain personal data. If in doubt your Manager will be able to advise on the Unit's retention periods.

Sixth Principle

- **Personal data must be processed in line with the data subject's rights. The rights of individuals are central to this principle:**

These rights include the following:

- The right of subject access lets individuals find out what information is held about them.
- Data subjects have a right to prevent processing that is likely to cause damage or distress to himself or herself or anyone else. They also have the right to claim compensation for damage and distress caused by someone breaking the conditions of the Act.
- Rights in relation to automated decision- making means that significant decisions should not be made about individuals using automatic processing alone.
- Individuals have the right to prevent processing for direct marketing – data controllers must not use personal data for direct marketing purposes if the data subject asks them not to.
- Individuals have the right to take action to correct, block, erase or destroy data that is inaccurate or contains opinions that are based on inaccurate data.

Exceptions

There may be situations in which these rights do not apply. For example, individuals do not have the right of subject access if it affects the way crimes are detected or taxes assessed.

Subject access may also be denied if the information requested involves disclosing personal data about a third party (that is another identifiable living individual) and he or she objects.

Seventh Principle

- **Appropriate security measures must be taken to protect against unauthorised or illegal data processing.**

Data controllers will make sure that security controls are in place and are followed. These may be technical (for example, relating to computer systems) or organisational (for example, management structures and the physical layout of the workplace).

Only employees who need to use personal data to carry out their work should have access to that data.

Eighth Principle

- **Transferring personal data outside the European Economic Area (EEA) is restricted unless the rights and freedom of data subjects are protected.**

Some countries outside Europe do not have the same legal requirements to protect information. The eighth principle means your employer or data controller must take steps to make sure personal data that is transferred outside the EEA is secure!

Data Collection – Use of Forms

The Board collects personal data about pupils, staff etc through the use of forms. The personal information being collected must be justifiable (see Principle No. 3) and clear as to 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

Some Board Units may 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 of the Act. The purpose of collecting this type of data should always be stated. 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 contact the FOI Unit.

The title on the form may already 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.

The statement can appear on the top or bottom of the form so that the data subject is made aware of the implications of their data being processed before they sign 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 Board 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.

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 (see Intranet for details of the Board's Notification); 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.

(a) 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 questions, which you believe only the data subject could answer, i.e. child's birth date, address, 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.

(b) 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, or a disclosure in the Board's Notification.

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.

You may need to check that the request has the consent of the data subject before releasing the information, for example, details of salary for mortgage application.

(c) 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.

(d) Tracing Disclosures

All disclosures should be traceable in order that any errors may be corrected. Systems should be in place to enable the manager to trace persons or organisations to whom personal data has been disclosed. A Data Subject is also entitled to this information when making a Subject Access Request.

Dealing with a Subject Access Request.

A data subject whose details are held by the Board, 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. **Subject Access Requests must be logged with the FOI Unit.**

They are then entitled to be told whether the Board, 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 from time to time, as set down 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.

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 (Educational records are covered by other legislation)
- 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 Board.

The FOI Unit can provide guidance on responding to subject access requests.

Notification – What is it?

What is notification?

- The Information 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.

Why does the Board need to notify?

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

How can I view the Board's Notification?

The Board's Notification details are published on the Board's Intranet

Or you can view the details on the Information Commissioner's website:

Changes to the Notification

If any Board Unit is processing, or intends to process, personal data for a purpose other than what is in the Board's Notification then the manager must contact the FOI Unit immediately so that amendments/alterations can be processed.

Remember: No Board Unit can process personal data for a particular purpose if that purpose has not be 'notified'.

Security of Personal Information

In the Workplace

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 Board 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. Remember you are responsible for your logon. Passwords should never be divulged to another person.
- ✓ CDs, disks, USB memory sticks, tapes, printouts and other storage media containing personal data should be stored securely 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/third party.
- ✓ 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.

Home Working

Some Board staff undertake work out of the office, for example, visits to schools, and it may involve the use of ICT equipment to record personal data. Similarly, paper files containing personal data may also be used away from the Office environment.

Permission should always be obtained before processing personal data out of the office environment 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 out of the office. This is likely to mean that computers are password protected and are not left unattended with personal data accessible. The Board's **Internet and Email Policy** and the **Computer Usage Policy** should be followed.

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 Board.

Extra care should be taken when transporting files to and from the office. 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!

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.

Managers are responsible for ensuring that their staff have received training and guidance on security of personal data/files, releasing personal data and dealing with subject access requests.

Heavy fines, to be paid personally by the individual/Board officer, 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 Board 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.

Frequently Asked Questions

Q: A manager 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: An outside fitness firm is setting up in the area and would like to mail-shot the staff. Can the Board issue names and addresses of staff?

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 staff, e.g. pension information attached to salary payslip.

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?

A: 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 staff 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 a staff/pupil who may have committed an offence. Can the Board/school 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 sample Form 81 page 30). Also, only give the officer what is necessary, not whole files or printouts relating to a pupil/staff. Personal information can be released but only if a crime is suspected or for the apprehension or offenders.

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 the child's records/information held eg statementing file. (Education (Pupil Records) Regulations NI 1998 refers) The age of the child should be considered when releasing information to parents. If the child is considered mature enough to understand the implications of data protection, then the parent may have to get the child's approval. There is no clear age definition and get request should be considered no a case by case basis.

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! The Board may have a statutory right to hold information that your service needs for administering the child's progress through the service and to disclose it within the terms of your notification and the provisions of the Act.

Q: An employee 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 officer to write a note authorising/requesting the release.

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.

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.

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

