Information Management Strategy
Support Materials for Schools

Data Protection and School Administration

In the collection, storage and processing of personal information regarding pupils the school is acting as 'Data Controller'. This means that the school must satisfy certain obligations in order to comply with the Data Protection Act 1998. Pupils, being the subject of the data held, are 'Data Subjects' and as such have rights, protected by the Act, with regard to the data held about them.

The list below is not intended to be exhaustive but to give a brief overview of obligations and responsibilities. Further detail on the use of the UPN and the law governing the use of personal data follows in this section. Additional information on the allocation and use of the UPNs is included at Section 1.

The School Must:

o Complete a **Notification** to be added to the register of data processors.

- Notification is a statutory requirement. Regulations now mean that the school (rather than the Head Teacher and Governing Body) can register.
- Notification must be updated annually.
- When any part of your entry becomes inaccurate or incomplete, you must inform us. This action must be taken as soon as practicable and in any event within 28 days of the date on which your entry became inaccurate or incomplete. Failure to do so is a criminal offence.
- A fee of £35 is payable for registration.
- You can complete the request for a notification form on line at www.ico.gov.uk. This should be faxed or posted to the Information Commissioners Office, marked for the attention of the Notification Department (Notification requests). Alternatively, the information can be emailed to (notification@ico.gsi.gov.uk).

o Issue a **Fair Processing Notice**

- A Fair Processing Notice sets out the data collected, how it is used and with whom it is shared.
- The Fair Processing Notice must be issued to every new pupil who joins your school.
- A template Fair Processing Notice for the Welsh Assembly Government, LEAs and Schools has been sent electronically to your

LEA for them to amend to local conditions and distribute to schools. All pupils joining a school should be given a copy of the notice.

- A template Fair Processing Notice is included at Section 5

- Ensure the security of data and the systems used to store and access it. More information on this is given in Section 4 of this pack.

- Respect the rights of individuals in relation to the data held on them. This includes responding appropriately to requests for access to personal records.

- Take all reasonable action to ensure that pupils, and where appropriate their parents, are aware of their rights in relation to personal data held on them. Section 5 provides some suggestions on how this might be achieved.

- Develop **Information Sharing Protocols**, where necessary setting out the conditions under which they provide information to others.

Pupil Rights

The Data Protection Act (1998) gives all individuals, regardless of age, the general right to find out what data is held about themselves by any "data controller" on computer and most paper records. Requests to see or receive copies of records are known as 'subject access requests' and should generally be made in writing to head teachers.

If an individual is incapable of understanding or exercising their own rights under the Data Protection Act, for instance because they are too young, parents or legal guardians may make subject access requests on their behalf.

Remember, there is no automatic right for a parent or legal guardian to have access to data held on children in their care. Further there is no mandatory age limit set for when a pupil may be deemed too young to understand, and therefore exercise their rights. However the presumption is that by the age of 12 a child has sufficient maturity to understand their rights and to make an access request themselves if they wish.

Each case/request should be considered on its own merits.

Data Protection and the UPN

The **Unique Pupil Number** (UPN) is:

> "a number that identifies each pupil in Wales uniquely, allocated to them according to a nationally specified formula on first entry to school, and intended to remain with the pupil throughout their school career regardless of any change in school or Local Authority (LA) or even where they move between schools in Wales and England"

More detailed advice about the issue and use of UPNs is provided in Section 1

The Welsh Assembly Government held discussions with representatives of the Information Commissioner in 2002. A particular concern was that if the UPN was widely known and displayed, then other organisations would become aware of it and might seek to use it for their own purposes. If use of the UPN were to spread it might provide the means for the collation of data about children and young people, possibly by commercial organisations for commercial gain, without any benefit to them of the educational system.

To help minimise the risk to personal privacy it was agreed that:

- The UPN be, **as far as possible**, a "blind number" held by schools on the pupil's electronic record, and only output when required to provide information to the LEA, the Welsh Assembly Government, another school when the pupil transfers or another official data controller. The UPN should **not** be regarded as an automatic adjunct to the pupil's name routinely appearing on any record or document relating to them (the pupil admission number should continue to be used for such administrative purposes). It is particularly important that the UPN is closely guarded as it relates to children and should therefore not be widely and openly displayed in a manner that could compromise their confidentiality.

Use of the UPN by schools

- Schools should not generally advise pupils (or parents) of their UPN, nor indeed take any positive steps to inform them of the introduction of the UPN system. Schools will of course wish to deal with any enquiries from pupils or parents honestly and without evasion, and pupils have the right under the Data Protection Act to receive on request a copy of any information the school holds about them (including their UPN). However, reflecting the Information Commissioner's Office concerns, particular care should be taken to prevent potential abuse of use of the UPN outside of its use in education as a general identifier. Thus, schools should not give out details of pupils UPN, other than as a result of a lawful and legitimate request.

- Schools should not enter UPNs on pupils' paper files or on any other physical documents, including admission and attendance registers, and

should continue to use the admission number, rather than the UPN, as a general pupil reference number with the school. Schools should store pupils' UPNs in their Management Information System (MIS) using accredited educational software packages. Storing UPNs electronically will minimise security risks and adhere to Data Protection requirements.

- Schools are advised that generally the UPN should not appear in printed format. In the event that this does happen then the printed document should be kept securely and shredded immediately to prevent inappropriate use or a breach of security.

Use of UPNs by other local agencies

The use of the UPN restricted to education related purposes imposes some limits on the extent to which other local agencies may have access to pupils' UPNs.

The UPN may only be passed to other persons in accordance to the Regulations governing this. Under the Education (Information About Individual Pupils) (Wales) Regulations 2007 (SI 2007 No. 3562 (W.312)) we understand the prescribed bodies to whom the UPN may be provided are Local Education Authorities, The Office of Her Majesty's Chief Inspector of Education and Training in Wales, The Local Government Data unit and Careers Wales companies. Additionally, persons conducting research into the educational achievements of pupils and who require individual pupil information for that purpose may also be provided with the information.

It should be noted that, in the case of looked after children, regulations now permit the transfer of individual pupil data (including UPNs) to the social service department of the local authority which looks after the relevant child or children whose data are being transferred ensuring that these children receive appropriate educational provision, and that their progress is monitored both individually and as a group. It would be legitimate to use UPNs to facilitate this exchange of information, but not legitimate for social services departments to go on from there to adopt UPNs as a general client identifier used for their own purposes whether education related or not.

The Data Protection Act: A Brief Guide

Introduction

The use of personal data has many benefits, however, whenever personal data are collected and used, people's lives can be adversely affected. It is vital that those who 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.

The Data Protection Act 1998 came into force on 1 March 2000. It sets out rules for processing personal information and applies to many paper records as well as those held on computers. Details of which paper records that act applies to can be found on the information Commissioners web site at www.ico.gov.uk/about_us/regional_offices/wales.aspx

The Data Protection Act in practice

The Data Protection act applies to 'personal data' that is, data about identifiable living individuals. Those who decide how and why personal data are processed (data controllers), and those who may carry out the processing on behalf of controllers (data processors) must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

The rules of good information handling – the principles

Anyone processing personal data must comply with the eight enforceable principles of good practices. They say that data must be:

1. Fairly and lawfully processed;
2. processed for limited purposes and not in any manner incompatible with those purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept for longer than is necessary;
6. processed in line with the data subject's rights;
7. secure;
8. not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intensions of the data controller towards the individual.

Processing personal data

'Processing' is broadly defined and takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed "fairly and lawfully". A data subject must be told the identity of the data controller and why that information is to be processed; these details are given in a 'Fair Processing Notice'.

Processing may only be carried out where at least one of the following conditions has been met:

- the individual has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- the processing in necessary to carry out public functions;
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

A template Fair Processing Notice for the Welsh Assembly Government, LEAs and Schools has been sent electronically to LEAs for them to amend to local conditions and distribute to schools. All pupils joining a school should be given a copy of the notice.

Security

Data controllers must take security measures to safeguard personal data. The 1998 Act requires that data controllers must take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of data. Where a controller uses the services of the data processor the security arrangement must be part of a written agreement between the two.

See section 4 of this pack for further advice on keeping information and administration systems secure.

Notification

Most data controllers will need to notify the Information Commissioner, in broad terms, of the purposes of their processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register. Notification is not linked to enforcement. Under the 1998 Act all data controllers

must comply with the data protection principles, even if they are exempt from the requirement to notify. Notifications are renewable annually.

The rights of individuals

1. *The right of subject access*

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

2. *The right of rectification, blocking, erasure and destruction*

   The Data Protection Act allows individuals to 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.

3. *The right to prevent processing*

   A data subject can ask a data controller to stop or request that they do not begin processing relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial distress to themselves or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request.

The above notes are based on extracts from guidance issued on the Information Commissions Website (www.ico.gov.uk)

The notes are intended for information purposes only and should not be assumed to cover all aspects of the Data Protection Act 1998

Further advice is available from you LEA Data Protection Officer or by contacting the Office of the Information Commissioner.