

A large circular inset image showing two women in a meeting. One woman on the left is wearing a blue top and a grey fur scarf, resting her chin on her hand. The woman on the right has curly hair and is wearing a light-colored top, also resting her chin on her hand. They appear to be looking at a laptop screen.

Data protection and security

a summary for schools





Recent legislation on data protection and freedom of information has given greater rights to the individual and alongside them, greater responsibilities on those who hold personal data, whether on paper or electronically. This document provides a brief overview of the implications these changes involve for schools.

Data Protection

Schools hold information on pupils and in doing so, must follow the requirements of the 1998 Data Protection Act. This means that data held about pupils must only be used for specific purposes that are allowed by the Act. The rules regarding personal data also apply to employees, whether they are teaching or non-teaching staff.

Schools are 'data controllers' under the Act in that they process 'personal data' in which people can be identified individually. When data is obtained from data subjects the data controller must ensure, so far as is practicable, that the data subjects have, or are provided with, or have readily available to them, the following information, referred to as the 'fair processing information':

- Details of the data that they hold on them
- The purposes for which they hold the data
- Any third parties to whom the information may be passed.

The DPA updated the rules and regulations on the protection of the individual and extended the principles to apply to all personal data that is processed. The DPA covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data and there are eight principles that must be adhered to as well as a number of conditions that apply. This Act has been extended to apply to paper files as well as electronic data, so the principles now apply to records and notes that are kept, for example, in teachers' mark books. The Data Protection Principles state that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than necessary
- processed in accordance with data subject's rights
- secure

In addition, data must not be transferred to other countries without adequate protection.

Each school that processes data must notify the Information Commissioner annually (originally it was 5 years) of that fact. If under the previous Act a school's governing body have registered in addition to the headteacher then, under the new Act, there need be only a single registration, and the double entry will need to be corrected.

Whilst all eight principles must be adhered to, two are highlighted here – the first and seventh.

Personal data should be processed fairly and lawfully

The two key words in this principle are 'fairly' and 'lawfully'. What do they mean for schools in practice?

The DPA sets out a 'fair processing' code. This requires data controllers to inform subjects about the purposes for which their personal data will be processed. This information should be provided at the time the personal



What procedures are in place to inform pupils about the purposes for which personal data is processed?

What procedure is followed for pupils who are too young, or unable, to understand?

data is obtained from the data subject, and should be comprehensive and transparent.

Problems may arise in providing this information for young children. The guidance is that as soon as children are able to understand their rights under the Act, they should exercise these rights on their own. The

Information Commissioner's guidance is that children by the age of 12 have sufficient understanding to make their own decisions, but there may be exceptions to this view.

'Lawfulness' can be broken down into two areas:

- The annual notification to the Information Commissioner needs to be comprehensive, setting out all the categories of personal data obtained, from whom it is obtained and to whom it is disclosed
- One of the conditions of Schedule 2 of the Act must be satisfied. The easiest way to do this is to obtain the data subject's consent to that processing. Consent will only be valid if the fair processing information has been provided. Ideally, consent recorded in writing is the most appropriate.

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

Those responsible for procuring and managing IT systems are most likely to be required to consider the technical measures to be taken against unauthorised or unlawful processing of personal data. What is appropriate will depend on the nature of the personal data being processed (including its sensitivity), the perceived risk of unauthorised or unlawful processing, and state the technical safeguards available to be implemented.

The DPA deals more specifically with the measures that must be adopted where a data controller uses a data processor to process data on its behalf. If, for example, a school outsources its IT maintenance and support function, the supplier will be a data processor for the purposes of the DPA.

The additional obligations placed on data controllers using data processors are that:

- the data controller must put in place a written contract with the data processor, obliging the data processor to take appropriate security measures in relation to the personal data it is processing
- the data controller must take reasonable steps to ensure compliance by the data processor with its security obligations; depending on the nature and volume of the personal data being processed on behalf of the data controller, 'reasonable steps' may range from requesting regular written updates from the data processor as to the security measures it is implementing, to full audits by the data controller involving visits to the data processor's premises.

Will the information about people that is passed on to content providers enable them to uniquely identify any individual teacher or pupil?

Does the school regularly audit the effectiveness of its internal security measures and those adopted by data processors where they are used?

What provisions are in place to keep up to date the publication scheme for all the information the school holds?



Using the internet and new technologies in schools

The internet can be an extremely valuable educational tool. As a source of information it is unrivalled, and through email, discussion forums and chat rooms, it offers new forms of communication too. However, there are three aspects of the internet (email, chat rooms and school websites) that, while they offer exciting opportunities for pupils, all present issues that must be addressed.

Schools, as with other organisations, have a right (and a duty in relation to pupils) to monitor use of their internet and email systems to prevent them being used inappropriately, for unlawful purposes or to distribute offensive material. However, an individual has a right to privacy. It is the duty of any organisation that provides access to the internet and email to balance these two separate rights and in the case of schools, different policies may prevail for staff and for pupils. In both cases, however, schools should be open on the subject of monitoring the use of the internet and email, and state under what circumstances individuals may use such systems for private communications. In a school, this can be achieved through the development of an acceptable use policy. Such a policy also needs to include use of the system to send offensive or bullying messages to pupils or staff and issues of security when accessing the school's intranet from outside the school via a mobile phone or PDA.

Email

Email can be a useful tool in the development of communication skills and extending the learning process. Students of foreign languages use email to correspond with native speakers abroad, for example, or to send and receive weather data across the world and pupils with special needs find email a valuable tool where letter writing or using the telephone would be impossible. However, there are a number of management implications of implementing email in school, and acceptable use of email by staff and pupils. Should all staff and pupils have their own mailbox, should staff email addresses be available to everyone, pupils and parents alike? Should pupils be able to send homework by email? Schools should have a policy in place that specifically addresses these, and related, issues.

Chat rooms

Chat is a way of communicating with others in real time over the internet in virtual meeting places called 'chat rooms'. Although mainly regarded as a leisure activity, chat rooms can also provide educational benefits. Pupils are able to chat with peers anywhere in the world, sharing experiences, comparing lifestyles or working collaboratively.

Within school, pupils should only be given access to educational chat rooms. They should be moderated to ensure that discussions are kept on topic and that

there is no bad language or inappropriate behaviour. Good chat rooms should have clear policies and privacy statements setting out acceptable behaviour, and these should be upheld and enforced. Guidelines for using chat in school should be included in an acceptable use policy.

As part of general safety for using chat rooms, pupils should be taught never to give out personal details that would identify who they are, and never to arrange to meet anyone they have 'met' in a chat room. Additionally, pupils should also be taught not to rely on anyone they have met in a chat room for important advice, and if anything makes them feel uncomfortable, not to reply to the message but instead seek advice from a teacher, parent or carer. Many children access chat rooms outside school and these chat rooms are likely to be unmoderated. It is essential that pupils are aware of these differences and taught safe and responsible behaviours whenever (and wherever) they are engaged in any communication in a chat room.

School websites

Many schools now have their own website, providing excellent opportunities for showing the range and breadth of work the school does, providing a source of information to parents, and developing links with the wider community. There are, however, certain safety issues that need to be considered:

- A school website should take care to protect the identity of pupils: where a child's image appears, the name should not, and vice versa
- Parental permission should be obtained before using images of pupils on the website.

If a school collects personal data in any form via its website this may be subject to data protection legislation; a clear and detailed privacy statement should be displayed prominently on the site stating how the information will be used. Schools should also take care to protect intellectual property on their site, and should not provide any information which could be in breach of copyright law.

Mobile technologies

The developments of mobile technologies such as phones (including camera phones) and PDAs have many benefits for the individual and to education. In addition to the standard services of voice calls and text messaging, the more advanced networks such as 2.5G and 3G provide:

- video messaging
- mobile access to the internet
- entertainment services (e.g. video streaming of sporting events)
- information-based services. Increasingly, schools need to include these devices in acceptable use policies

Passing on information

What procedures are in place for safe disposal of the school's data and computer equipment?

Schools hold information about children and adults and they process it in a number of ways to improve the quality and standard of their provision. Information is passed electronically from schools to LEAs (pupil transfer data, for example) and examination boards. LEAs pass information to a number of statutory bodies (such as QCA and Connexions), and to contractors who provide other services (content providers). Additionally, the Children and Young People's Unit (CYPU) requires local authorities, where necessary, to share information with other local government partners to identify children and young people in danger of social exclusion.

The implementation of connecting Regional Broadband Consortia and LEA networks (*interconnect*) to form a national education network has potential for delivering many services and resources. In addition to the many benefits this brings, particularly in sharing educational content, there is the challenge of ensuring that only those authorised to use a resource are able to do so.

This requires a set of standards for inter-organisational authentication, authorisation of users and accounting of which resources are used, that can be applied by all concerned. To achieve this, information about individuals needs to be made available to the content provider who may be another LEA, RBC or a third party providing a service.

Keeping personal data secure

All personal data needs to be kept safe and made available only to those who are authorised to access it, and this raises a number of issues:

- The first is compliance with the Data Protection Act (DPA) which requires annual registration by schools and LEAs regarding the data they collect and keep and how they use it.
- Secondly, information is passed to third parties who are contracted to provide services for schools. The DPA requires those who own the data and pass it to others to ensure that measures are in place for its safety and integrity and that it is not used for any purpose other than that for which it was collected, as well as how it will be destroyed when it is no longer required.
- In order for the educational network (*interconnect*) to function properly, information will need to be passed from one place to another. What information should be passed on, what information should be held by whom and where it will be held so that individual pupils are not identified is the challenge. The DfES is currently undertaking an authentication, authorisation and accounting project (AAA) that will

recommend the standards that should be applied. This project is expected to report towards the end of March 2004.

- The CYPU requires local authorities to have an Identification, Referral and Tracking (IRT) strategy for children and young people who are at risk of social exclusion. The implications for schools and LEAs in passing information to other schools and LEAs, and the LEA to local government partners, raise important questions. Issues of whether to do so, how much information to pass on and when to pass the information have been highlighted in the wake of the Victoria Climbié case. A number of local authorities have received funding to develop systems for IRT that will ensure that no child, after being identified as being at risk, subsequently 'falls through the net'. The outcomes of these trailblazer projects are expected at the end of the 2003/4 financial year.

Safe disposal

An aspect of data security that can be overlooked relates to the disposal of computing equipment. Schools have legal responsibilities for the personal data which will be on hard disks (including things like email and passwords). Just deleting files or even formatting the disk is not sufficient since widely available software programs can recover some or all of the information. Schools are advised to check that the organisation to which any equipment may be given will provide a warranty that they also securely erase all disks. It is advisable to consult your local technical support for advice in these areas.

If the disks contain particularly sensitive information, then the industry recommendation is that they should be physically destroyed by fire or smashing them.

Are there regular reviews of access levels and password controls to ensure that only those people and departments entitled to it have access to personal data?



The School's Legal Responsibilities

A school, like every other data user, must conform to the requirements of the Data Protection Act (1998). In particular this requires the school to formally notify the Office of the Information Commissioner of:

- the purposes for which the school holds personal data
- what data it holds
- the source of the data
- to whom the data is disclosed
- to which countries the data may be transferred.

Under the Act, each school is a separate data user and must complete a notification each year. The LEA may wish to provide advice and guidance here but it is not clear if it has a legal responsibility to do so.

The keeping of personal data covers facts and opinions relating to an individual. It also includes information regarding the intentions of the data controller towards the individual and the action that will follow the processing. For example, altering, destroying, disclosing, disseminating, obtaining and holding, together with a number of other actions, are all incorporated in the concept of processing.

Schools retain files containing personal data on computer systems. However, there is some debate about how long such data should be retained after pupils have left school or employees have moved on. Within the 1998 Act the Fifth Principle states:

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

As a general rule of thumb, a school must look at its original Notification under the Act and check on the stated purposes for which it is holding data. Each of these could then point to an appropriate length of time, for example:

- Finance Data – 6 years or as laid down by LEA Financial Regulations
- Pupil and Staff Data – 7 years seems to be an acceptable period, after which a school might not be required to provide exam results or references.



The Freedom of Information Act 2000

This Act gives a general right of access to all types of 'recorded' information held by public authorities, sets out exemptions to that right and places a number of obligations on public authorities. It will be brought fully into force by January 2005. Public authorities will have two main responsibilities under the act:

- They will have to produce a 'publication scheme' (effectively a guide to the information they hold which is publicly available)
- They will have to deal with individual requests for information.

The duty to adopt a publication scheme came into force for local authorities (28th February 2003) and for schools

and other educational institutions (29th February 2004).

Individuals already have the right to access information about themselves, held on computer, and in some paper files, under the Data Protection Act 1998.

As far as public bodies are concerned, the Freedom of Information Act will extend these rights to allow access to all the types of information they hold, whether personal or non-personal. Requests for information will have to be made in writing and this includes email. However, the public authority will not be required to release information to which any of the exemptions applies. These exemptions revolve around the test of prejudice and that of public interest.

External access and transfer

Much progress has been made in the development of infrastructure and the development of computer systems. At the same time, the legal requirements on schools and LEAs to pass on and receive information from DfES, QCA, Ofsted and other bodies have brought a new dimension to the use of ICT. The advantages to education of such communication are immense, but there are a number of areas for concern, including unauthorised access to information held on computer systems. Transferring information across computer networks also creates the need to ensure the integrity of the data being transferred and that the identity of the individual is secure. There are technical solutions to these problems, yet hackers are always striving to find new ways to breach computer systems, so schools need to be ever vigilant.

Increasingly, as schools develop intranets and extend access to them for staff and pupils at home, there is a need to ensure that the school's system is safe and that visitors can only access information appropriate for their use. A firewall and/or password-protected system that prevents pupils and others from accessing personal or financial information is essential.

Used in an educational context, these features can enrich the curriculum but they may pose risks for pupils that should be included in the school's internet safety education programme. The dangers associated with a standard PC regarding unsuitable material apply to mobile phones and other devices too, yet because mobile phones are personal and private devices, it is not always possible for parents or schools to monitor their use. The indications are that mobile phones and other devices will be more readily available and any policy on internet safety will need to include mobile technology. Further information on such devices can be found on the Superhighway Safety site.

Checklist for schools

- Does the school have an Acceptable Use Policy (AUP) that is regularly updated to take account of emerging technologies?
- Is pupils' use of the internet, email and/or chat rooms regularly monitored to ensure that inappropriate use is not being made? Are sanctions in place where pupils access inappropriate sites or post bullying or offensive messages?
- Does the school send information to parents regarding ICT use in schools?
- Have pupils and parents/carers (where appropriate) given their consent for children to use the internet in school? What action will the school take if consent is withheld?
- Does the school have filtering systems in place to prevent pupils from accessing inappropriate materials? Are there procedures in place for pupils to report accidental access to inappropriate material?
- Does the school adopt safe practices regarding the publication of the images and names of pupils and staff on its website?
- Does the school take reasonable measures to monitor the use of emails by pupils and staff?
- Does the school provide appropriate opportunities within a range of curriculum areas to teach internet safety?
- Are there procedures in place to deal with 'disclosure' by a child of a personal nature as a result of internet safety education? Has the school nominated a member of staff who has responsibility for such issues?



Are security measures reviewed regularly against the perceived risks and the latest technology available?

Useful information

Further guidance and information on data security and data safety can be obtained from the following sources:

Essential sites

Superhighway Safety
<http://safety.ngfl.gov.uk/schools>

GridClub for pupils and teachers
<http://www.gridclub.com>

Building the Grid
<http://buildingthegrid.becta.org.uk>

Bullying online
<http://www.bullying.co.uk/>
http://www.besafeonline.org/English/bullying_online.htm

Sample policy documents
<http://www.kented.org.uk/ngfl/policy.html>

Other useful sites

Information Commissioner
www.informationcommissioner.gov.uk

TeacherNet – data protection
www.teachernet.gov.uk/management/tools/ims/dataprotection/

JISC Data Protection Code of Practice for the HE and FE sectors
www.jisc.ac.uk/index.cfm?name=pub_dpacop_0101

Local Government Information House
www.idea-infoage.gov.uk/

Connexions
<http://www.connexions.gov.uk>

Data Protection Act 1998
<http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm>

Freedom of Information Act
<http://www.legislation.hmso.gov.uk/acts/acts2000/20000036.htm>

Computer Society – disposal of computers/disks
<http://computer.org/security/v1n1/garfinkel.htm>

Data Protection Act Terminology

The following terms are used in the Data Protection Act:

- **personal data** – data relating to any living individual, or from which a living individual can be identified; this can take the form of electronic or manual records as well as photographic and CCTV images
- **sensitive personal data** – personal data relating to an individual's mental or physical health, race/ethnic origin, religious or political beliefs, sex life or trade union membership
- **data subject** – an individual to whom any personal data relates
- **data controller** – any organisation that is responsible for processing personal data
- **data processor** – any organisation that processes personal data on behalf of a data controller

Becta is grateful to Scott Wagland of Eversheds, for his contribution to this document



Millburn Hill Road
Science Park
Coventry CV4 7JJ

Tel: 024 7641 6994
Fax: 024 7641 1418

Email: becta@becta.org.uk
URL: <http://www.becta.org.uk>

© Copyright Becta 2004

You may reproduce this material, free of charge in any format or medium without specific permission, provided you are not reproducing it for profit, material or financial gain.

You must reproduce the material accurately and not use it in a misleading context. If you are republishing the material or issuing it to others, you must acknowledge its source, copyright status and date of publication.

While great care has been taken to ensure that the information in this publication is accurate at the time of publication, we accept no responsibility for any errors or omissions. Where a specific product is referred to in this publication, no recommendation or endorsement of that product by Becta is intended, nor should it be inferred.