Data Protection for Schools
Compliance Checklist

Here is a simple “bullet point” list of actions your school should take to work towards compliance with the Data Protection Act. It is a non-exhaustive list, designed as a foundation to build upon.

For further advice or for information about our tailored training for schools please visit our website www.theinformationlawpractice.com or contact us: training@theinformationlawpractice.com telephone 01386 793632.

1. Notification of Data Processing

Your school is a data controller of personal data and is legally required to annually NOTIFY the Information Commissioner’s Office (ICO). Notification is the process by which a data controller gives the ICO details about their processing of personal information.

Notification is an annual requirement currently costing schools £35 per year. Failure to notify when required to do so or to keep a notification up to date is a criminal offence. If convicted your school faces a fine, a criminal record and adverse publicity.

Our Tips

- Implement an annual automatic diary reminder to ensure you do not forget to file your notification.

- You may be able to use a notification template specifically written for schools. These templates are available on the ICO website www.ico.gov.uk

2. Comply with the 8 Data Protection Principles

As a data controller your school must process all of its personal data in accordance with 8 enforceable Principles. A summary of the 8 Principles is set out below.

Principle 1:
Process data fairly and lawfully and only in the circumstances set out in the Data Protection Act.
Example: Principle 1 requires you to issue all pupils with a Fair Processing Notice explaining who the data controller is (i.e. the school), the purposes for collecting their personal data and anything else needed to ensure fairness. E.g. who you share personal data with outside the school such as the DCSF, the LEA, Ofsted, Connexions etc.

**Our Tips:**

- **The DCSF has issued standard template Fair Processing Notices for you to use.** The templates and a detailed guide on how to use them can be obtained from [http://www.teachernet.gov.uk/management/ims/archive/arcdatamangmnt/fpnpu_pils09/](http://www.teachernet.gov.uk/management/ims/archive/arcdatamangmnt/fpnpu_pils09/)

- **But remember these are just templates. If your school carries out data processing activities which are not covered in the template such as running biometric systems for cashless catering, registration and library book borrowing, you will need to amend the template accordingly.**

- The DCSF also produces template Fair Processing Notices for data subjects other than pupils, i.e. staff and other adults. Click on this link for more information [http://www.teachernet.gov.uk/management/ims/archive/arcdatamangmnt/fpnsw_f09/](http://www.teachernet.gov.uk/management/ims/archive/arcdatamangmnt/fpnsw_f09/).

**Principle 2:**
Process data for the purpose originally specified and not for unrelated purposes.

**Principle 3**
Personal data should be adequate, relevant and not excessive

Example: Don’t take more personal data from job applicants than you really need.
Principle 4  
**Personal data should be accurate and up to date.**

Example: Ensure that you regularly update your pupil contact data. In doing so, remind parents and carers that they should notify you immediately of any changes to contact information. The onus is on the school to keep its database up to date but providing you have taken reasonable steps to do so you will not be in breach of this Principle.

Principle 5  
**Don’t retain personal data for longer than necessary**

We are often asked by schools how long they should keep records for. The answer to this question depends upon the nature of the individual document. In some cases, statute will require a school to retain a document for a particular period. For example, secondary pupil files should be retained for 25 years following the pupil’s date of birth after which they should be securely shredded. This is in line with the Limitation Act 1980 which provides that individuals have 25 years to bring a claim against a school. In other cases, official guidance or Codes of Practice may stipulate how long a document should be retained. For example, pre-employment vetting records (including CRB checks) should be retained for 6 months after the date of the check, in line with CRB Guidelines. In other cases, the school may have a genuine operational reason to retain a document for a certain amount of time. In other cases, there are no legal or operational reasons why a document should be retained, in which case these documents should be securely disposed of.

**Our Tip:**

- The Records Management Society of Great Britain has produced a Retention & Deletion Schedule specifically for school records. You can use this free of charge by visiting [www.rms-qb.org.uk](http://www.rms-qb.org.uk)

Principle 6  
**Process personal data in accordance with data subjects legal rights.**

Data subjects have several legal rights under the Data Protection Act which, when exercised, may enable them to “control” the way in which your school processes their personal data.

For example, the right of subject access gives data subjects the right to ask the school for a copy of their personal data. This is known as a Subject Access Request or SAR for short. Most SAR’s will be made by a pupil or someone acting on their behalf. However, remember that staff, governors and parents can also ask the
school for their personal data. If the request involves information held in an “educational record” the school will have just 15 school days to process the request. However, the clock does not start to tick until you have received the request in writing; received evidence of the data subject's identity, received the appropriate fee (for educational records this ranges from £1-£50 depending on the number of copies) and have been provided with sufficient information from the data subject to locate the information. Note that in some cases, due to the operation of legal exemptions, the data subject will not be entitled to receive some or all of his records. E.g. third party personal data, legal advice to the school, examination marks before they are published etc. For more information on how to handle a SAR you should take legal advice or attend a training course for schools. Please check our website regularly for details of our latest training courses for schools.

Maintained schools should also remember that parents of pupils also have a legal right to access their child’s “Educational Record” under the Education (Pupil Information) (England) Regulations 2005. This right is entirely separate to the pupil’s right of access under the Data Protection Act.

**Principle 7**

**Keep Personal Data Secure**

Principle 7 of the DPA requires you to take steps to prevent personal data from being accidentally lost or destroyed or from being used without authority. In deciding what security measures to implement the school can have regard to the cost of those steps and the state of technology. However in all cases, the more sensitive the personal data to be protected, the greater the security it deserves. For example, medical data.

**Our Tips**

- **Staff Training:**

  Principle 7 requires that all staff that handle personal data in schools should be reliable. This means that everyone in school that handles personal data should all receive at least 1.5 hours basic data protection training. Training needs to be kept up to date and documented. Ideally there should be one member of staff who has received detailed data protection training who can act as your Data Protection Officer.

**STOP PRESS:**

The Information Law Practice has trained hundred of schools in data protection and now also offers 1.5 hours on - site basic training for all staff at a date convenient to you. (Ideal for training large numbers of staff at a cost effective rate) For more information contact us on 01386 793632 or email us at training@theinformationlawpractice.com.
Organisational Steps:

- Read the BECTA report “Good Practice in Information Handling in Schools – Keeping Data Secure, Safe and Legal” and also it’s accompanying sub reports. Implement as many of the reports’ recommendations as you can afford. Download your copy by clicking here: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_dp_03&rid =14734

- Implement a data protection policy (or similar) which includes a policy for responding to data security incidents. Your Council may have one you can use. If not, consider the incident response guidelines produced by GovCertUK (the body responsible for Computer Security Incidents in the UK). Visit http://www.govcertuk.gov.uk/pdfs/incident_response_guidelines.pdf

  If you do suffer a data incident, being able to say that the school has a data security policy will be better than nothing.

- Appoint a member of staff to the role of Data Protection Officer/Information management Officer etc

- Home Working/Off Site Working Policy: Personal data processed on non school equipment is more difficult to regulate and protect. In particular it is prone to non - authorised access such as by a relative or friend of the authorised member. Home Working Policies should explain the steps staff must take to protect school data being processed either on home equipment or away from school. Ideally, staff employment contracts should contain contractual obligations to process school information in accordance with the school data protection policy and or home working policy. Your policy should also include post contract provision for the deletion of school data held on personal computing devices and the return of school storage devices.

Technical Steps

- General: Use password protection as standard; encryption of all sensitive or confidential personal data; restricted access to sensitive or confidential personal data; computer virus protection and use of firewalls; consider what level of internet access you allow staff and whether internet access represents a risk to the security of your IT systems; consider the steps you take in disposing of data. We recommend that all personal data is securely shredded and not put out with ordinary waste for collection; remove all data including personal data from
computers and other IT equipment that is capable of storing data, which are to be disposed of; consider risk management procedures to recover data (both automated and manual) which may be damaged or lost through human error, computer virus, network failure, theft, fire, flood and other disaster.

- **Encryption**: All laptops, USB storage devices (e.g. memory sticks) and other mobile computing devices that access or store personal data should use data encryption software. This should apply to both school owned devices and any non-school owned devices which are used for school work. For guidance on which encryption technology to use and how to install it refer to the BECTA report “Good Practice in Information Handling in Schools” and the accompanying “Data Encryption Good Practice Guide”. Click here to download your copy: [http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf](http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf)

- **Secure Remote Access**: The Becta report “Good Practice in Information Handling in Schools: Secure Remote Access” recommends that when data is required by an authorised user from outside school, e.g. A teacher working at home, access must be via secure remote access (e.g. two-factor authentication to the management information system). Becta outlines a number of solutions that schools can use to allow users to access sensitive or personal data from outside school, including using Shibboleth via the UK Access Management Federation for Education and Research, and use of the forthcoming Employee Authentication Service for two-factor authentication.

The guide also explains how schools can reduce the need for two-factor authentication (such as hardware token) by careful selection of the types of data that can be accessed remotely. For example, the type of data that schools make available online to parents should not be sensitive enough that it will require parents to be issued tokens.


- All manual personal data should be stored in locked cabinets. Particularly sensitive or confidential data should be subject to restricted access and kept separately, perhaps in a sealed envelope labelled accordingly.

- Some schools outsource processing of personal data to an external organisation (known as data processors) e.g. music therapists or teachers, Payroll function, IT support etc. If you contract with a data processor ensure you have a written contract with them that requires them to keep personal data safe and secure and to only process it upon the school’s instructions. Failure to ensure this means the school is in breach of Principle 7 (If you require help with these contracts, contact your legal department or call us on 01386 793632).
Principle 8:
Do not transfer personal data outside the European Economic Area unless the destination country can adequately protect personal data

Example: Schools websites that contain personal data may well engage Principle 8. You can comply with Principle 8 by obtaining the data subjects consent for their details to be posted on your website. This applies to pupils as well as individual staff members.

This checklist is related to data protection only and not child protection. Because you must also have regard to your child protection responsibilities, you should seek separate advice from an appropriate professional to ensure that your website does not prejudice the welfare of children. There may be child protection reasons why a pupil's details ought not to be posted on your website.

3. CCTV

If your school uses CCTV to routinely capture images of individuals then your system must comply with the Data Protection Act. I.e. include it in your annual notification and comply with the 8 Principles.

If your system is small and non-sophisticated and you will only be sharing the images with the Police for crime prevention purposes then you may need only comply with part of the Code of Practice (see Appendix 2 to the Code). However, if you use images for purposes other than those set out in the checklist e.g. for monitoring staff and pupils then you will need to comply with the Code of Practice in its entirety.

Our Tips

- The ICO Code of Practice lists all the things you must do to ensure your CCTV system complies with the Data Protection Act. Print a copy off for the member of staff responsible for managing the system.
- Decide up front the reason for installing CCTV. Is it for crime prevention and public safety or is it also to monitor car park infringements, non-school attendance etc? The purpose for installing CCTV needs to be communicated to pupils, staff and visitors in appropriately worded and placed signage.
• Signage must inform data subjects that CCTV is in operation for the purposes you have determined (e.g. crime prevention and or public safety) and to tell people who the data controller is (i.e. your school). Your signs should be placed where visitors can easily see them. E.g. at entrances. Signage is equivalent to a fair processing notice and helps you comply with the fairness requirements of Principle 1.

4. Dealing with Police Requests for Personal Data

From time to time your school may be asked to provide the Police with pupil information in order to help them investigate alleged criminal offences. Often these requests are expressed to be urgent and can have the effect of making the school feel pressurised into cooperating without properly checking out the legal position. So what exactly is the legal position?

Firstly, the school as data controller has a legal duty of non disclosure. In other words it should not disclose pupil data to third parties, including the Police unless it can claim a legal exemption from this duty. However, there is a relevant legal exemption within the Data Protection Act which can allow the school to disclose relevant personal data. However, in order to be able to claim this exemption the school must satisfy itself that the disclosure is necessary for the purposes of the prevention and detection of crime and by withholding the data the school would be prejudicing those purposes. (This is sometimes called the Section 29 exemption).

Schools should remember that the Section 29 exemption gives them a power and not a duty to disclose the data to the Police. In other words, the school does not have to claim the exemption and can instead insist on the Police obtaining a court order compelling them to disclose. However, in most cases, schools will want to cooperate with the Police and help them in anyway they can, providing of course that in doing so they do not breach the Data Protection Act.

Our tips

• Ask for the Police request to be put in writing and signed by a senior officer.
• The written request should specify the information sought and confirm that it is required for the prevention and detection of crime.
• If in doubt seek legal advice

This document is for general guidance only and does not constitute specific legal advice. It may not be up to date and is not designed to be comprehensive. You are advised to take specific advice from an appropriate professional in relation to specific situations.