CHILDREN, FAMILIES & EDUCATION DIRECTORATE

DATA PROTECTION

GUIDANCE FOR STAFF

INDEX

	Page no.
Data Protection Act 1998	3
Key Definitions	3
Data Protection Principles	4
Conditions for Processing Personal Data	5
Conditions for Processing Sensitive Personal Data	5
Notification	5
Individuals' Rights	6
Checklist before Processing Data	7
Fair Processing Information	7
CCTV	8
Security	8
Disclosure of Personal Data	9
Subject Access Request	10
Third Party Processing	11
Offences	11
How DP effects schools	11

Data Protection Act 1998 (DP Act)

The DP Act came into force on 1 March 2000. It is a law that protects personal privacy and upholds individual's rights. The Act applies to anyone who handles or has access to information about individuals.

All staff must be aware of and ensure they comply with the requirements of the Act.

Failure to comply with the Act could lead to criminal prosecution, claims for compensation by data subjects and disciplinary procedures.

This document is intended to assist staff in gaining a better understanding of the Act. The information contained in this document is based on guidance published by the Information Commissioner available on the website at http://www.informationcommissioner.gov.uk/

Key Definitions

Personal Data - means that the information is about an identifiable living individual. It includes both **manual** and **electronic** records.

It can be factual i.e. date of birth, or it can be an opinion i.e. how a manager thinks an employee has performed at an appraisal.

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.

Processing - any activity that involves the data i.e. collecting, recording, using, retrieving, storing, updating, disclosing or destroying the data.

Data Controller - a person or organisation who processes the personal information.

Data Subject - the person the information is about.

Data Processor - any person or organisation that process information on behalf of a data controller.

Information Commissioner - the person appointed by the Government to administer the provisions of the Data Protection Act.

Data Protection Principles

The Act is based on eight principles or rules for 'good information handling', which must be adhered to.

In summary, the data must be:

1. obtained and processed fairly and lawfully and, in particular, shall not be processed unless:

    - At least **one** of conditions in **Schedule 2** is met, and
    - In the case of **sensitive personal data**, at least **one** of the conditions in **Schedule 3** is also met."

    (See below for schedule 2 and 3 conditions)

2. held only for specified purpose(s)
3. adequate, relevant and not excessive
4. accurate and kept up-to-date
5. held no longer than necessary
6. processed in accordance with the rights of the data subject
7. subject to appropriate security measures
8. only transferred to other countries that have suitable data protection controls.

(Schedule 2) Conditions for Processing Personal Data

To comply with the first principle, at least **one** of the following conditions **must** be met before you can begin processing. Most likely conditions to consider will be:

- The data subject has given consent
- The processing is necessary for the performance of a contract between KCC and the data subject
- The processing is necessary for compliance with any legal obligation to which KCC is subject (not a contract)
- The processing is necessary in order to protect the vital interests of the data subject (for life or death situations)
- The processing is necessary to pursue legitimate interests of KCC or third parties.

(Schedule 3) Conditions for Processing Sensitive Personal Data

There are strict conditions for the processing of sensitive personal data. At least **one** of the conditions in **schedule 3 must** be met, together with at least **one** of the conditions in **schedule 2.** The most important conditions will be:

- The data subject has given their explicit consent (in writing and required for every separate occasion)
- The processing is necessary to comply with employment law obligations
- The processing is necessary for legal proceedings, obtaining legal advice or exercising/defending legal rights
- The processing is necessary for equal opportunities monitoring

Notification

To comply with the principles of the Act every Data Controller (including Schools) must register their reasons for processing personal data with the Information Commissioners Office; this process is called Notification. Failure to notify is a criminal offence.

The Information Commissioners Office maintains a public register of Data Controllers together with their purposes for handling personal data.

Managers have a responsibility for ensuring that all processing of personal data by their Unit/Team is covered by the KCC Notification.

Details of the KCC Notification can be obtained from the directorate Data Protection/Freedom of Information Co-ordinator. We must not hold personal data for reasons other than those specified in our Notification.

Individuals' Rights

The act also gives rights to the people the data is about. These rights are called 'subject access rights'.

Individuals are entitled to:

- be informed about any data held and the purpose(s) for which the data is being processed, i.e. subject access requests (**see Subject Access Requests**)

- prevent processing that is likely to cause damage or distress to themselves 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. Important decisions should not be made about individuals using automated processing alone (job-selection procedures such as psychometric testing and CV scanning)

- prevent processing for direct marketing purposes

- have any inaccurate information held about them corrected, removed or destroyed

- request an assessment by the Information Commissioners Office to determine if any part of the Act has been contravened.

Checklist before Processing Data

Before processing personal data staff should consider:

- Is it necessary to record this information?
- Is the purpose for processing covered by the KCC Notification?
- Is any disclosure covered by the Notification?
- Has the data subject been told that this information will be processed and why? (fair processing notice)
- Is the information non-sensitive or sensitive?
- If non-sensitive, do we have data subjects consent
- If sensitive – do we have explicit consent (in writing and required for every separate occasion)
- Is the data accurate?
- Is the data secured? **(see section on Security)**
- If you are processing personal data on behalf of another data controller for example, the police, fire or probation service, you should process their data only in accordance with their instructions.

Fair Processing Information

Whenever personal data is collected, you must provide the data subject with information about your intentions with their data, this is known as a fair processing notice.

You must inform the data subject of the identity of the Data Controller (KCC or School), the purpose(s) for which the information is to be used and with whom the information may be shared.

The data subject should be given the opportunity to opt out of having their data used for other purposes. This can be achieved by use of an opt out 'tick box'.

A list of individuals who have opted out should be kept and checked whenever necessary. If an individual receives information after specifying that they do not want it, the Act has been breached.

Example of a fair processing notice:

"Kent County Council is a data controller under the Data Protection Act 1998 and will comply with the requirements of the Act at all times. We will ensure that your information is treated in confidence and used solely for the following purpose(s) ……....."

There is an example of a fair processing notice for schools available on ClusterWeb via the following link:
http://apps.clusterweb.org.uk/forum/messages/594/596.html?1093951058

CCTV

If you operate CCTV or similar surveillance equipment in any location you are likely to be subject to the provisions of the Act. The Information Commissioner has produced a code of practice for users of CCTV, which is available to download or view from the website http://www.informationcommissioner.gov.uk/.

Security

All personal data whether manual or electronic must be kept secure to prevent accidental loss, damage or destruction. The extent of the security measures required will depend on the sensitivity of the data.

Paper records should be locked away in desks, filing cabinets or cupboards when they are not in use. The keys should be kept in a safe place.

If the data is electronic, access should be password protected. Do not share your user ID or passwords (as stated in KCC contracts). Ensure that your PC screen cannot be viewed by unauthorised personnel and log out of PC's when not in use, or lock PC using the Ctrl, Alt and Delete keys.

When records containing personal information have reached the end of their life, disposed of by shredding, incineration or using confidential waste bins.

Personal data should not be sent using a fax machine unless it has first been made anonymous (masked) or the fax machine is a 'safe haven' machine (in a secure area, which is locked when unattended).

Personal data should not be sent by email as its security cannot be guaranteed. We are currently looking into methods of encrypting the email system, which once achieved will allow staff to send personal data without worry of the data being viewed by unauthorised personnel. If it is necessary to send information in this way, make sure it has been anonymised first or send the data as an attachment to the email and flag as confidential.

If you are required within the course of your duties to take personal data home (including laptops, videos, etc.), do not leave the information unattended for any length of time, especially in a vehicle overnight. It is not recommended that home computers are used for the production of KCC documents, particularly when individuals can be identified and the data about them may be sensitive. Personal PCs should only be used if they have up to date virus protection software installed on them.

Using a personal internet service provider to send documents to KCC is to be discouraged. Personal or sensitive data should not be sent from home using personal email facilities as the security of the data cannot be guaranteed.

When transferring personal data to other parts of the organisation it is preferable for the files to be delivered in person. If personal data is to be sent externally ensure the information is made secure and clearly marked 'Confidential' and where possible use registered post or courier service to transport the data.

At all times treat peoples personal information as you would wish your own to be treated.

Disclosure of Personal Data

Staff must not disclose personal data to anyone unless legally required within the course of their duties.

All disclosures must be in accordance with KCC's notification and/or with the consent of the data subject. If consent is required and has not been obtained, disclosure can only take place if the personal data has been anonymised.

Where disclosure is permitted, always take appropriate action to ensure the identity of those you disclose to. Disclosure over the telephone should be discouraged, invite the caller to put the request in writing. If the request is urgent, take the caller's name and telephone number and verify their details before responding.

If a member of staff is in any doubt about disclosure they must seek advice from their Line Manager or the Data Protection/Freedom of Information Co-ordinator. Unauthorised disclosure of personal data may be a disciplinary offence.

Subject Access Requests

Requests for subject access must be made in writing, including email and should be completed within 40 days of receipt of the request (this differs for pupil education records – **see section How Data Protection effects Schools**). KCC currently charge a fee of £10 for dealing with a subject access request.

It is important that staff know how to recognise a subject access request and realise that it must be dealt with urgently. The request may not mention the Data Protection Act, it may just say 'I want to see all the information you hold about me'. Any member of staff who receives a subject access request must immediately contact the Data Protection/Freedom of Information Co-ordinator and provide details of the request.

KCC has an 'Open file policy' for staff wishing to see personal information held about them, contact Personnel for more information.

Third Party Processing

Where a third party processes personal data on behalf of KCC, e.g. payroll provider, web site hosting, analysis and reporting services, KCC must include in the contract these requirements:

- Choose a data processor providing sufficient guarantees in respect of the security measure they take
- Take reasonable steps to ensure compliance with those measures
- Ensure that processing is carried out in accordance with a written contract under which the data processor is to act only on instruction from KCC

- The contract must require the data processor to comply with obligations equivalent to those imposed on KCC.

Personal data must not be transferred to a country outside of the European Economic Area (EEA) unless that country ensures an adequate level of protection. If you are required to deal with such arrangements seek advice from the Data Protection/Freedom of Information Co-ordinator.

Offences

Failure to comply with the requirements of the Act could result in Council employees being held liable for their actions. The Act also makes provision for the separate personal liability of directors in respect of the offences committed by a corporate body. Where prosecution occurs in the Magistrates Court an offender is liable to a maximum fine of £5000, whilst in the Crown Court an unlimited fine may be imposed.

An individual who suffers damage or distress as the result of any breach of the requirements of the Act by a Data Controller, is entitled to seek compensation through the Courts.

An individual who believes they have been affected by the processing of personal data, may ask the Information Commissioner to assess whether or not the processing of the data has been carried out in compliance with the Act.

How Data Protection effects schools

Schools are legal entities (Data Controllers) in their own right as they collect and make decisions about the use of Personal Data, i.e. details of staff, pupils and parents or carers. Each school **must** therefore comply with the DP principles and register their processing with the Information Commissioner (Notification).

An application for Notification can be made either via the Information Commissioners website http://www.informationcommissioner.gov.uk/ or by telephoning the Notification Department on 01625 545740. The fee for notification is £35 payable annually. Reminders will be sent directly to schools. Both methods of registering will allow you to use a standard template, which has been designed to cover your specific activities. If

you choose to use one of the templates the details provided should still be checked, and any amendments made as necessary.

You do not need the help of an agency to notify on your behalf. Organisations throughout the UK have been troubled by bogus data protection notification agencies. The Information Commissioner is the only statutory authority for administering and maintaining the public register of Data Controllers.

The DP Act gives all school students, regardless of age, the right of access to their pupil records.

The Information Commissioner has stated that children who are old enough to understand what is being asked of them should be given the opportunity to give their own consent with regard to Data Protection issues. This is because the DP Act applies to people of all ages, not only those 18 and over. Although no guidance has been given as to how to prove that a child understands what is being asked of them, there is a legal case which set a precedent (Gillick v. West Norfolk and Wisbech Health Authority). This established that once a child becomes 12 years of age he or she is likely to be able to understand the implications of what is being asked. This is commonly referred to as the 'Gillick Principle'.

In light of this, if your school has children of this age, the Headteacher may be required to judge whether a child is 'Gillick Competent' or not and whether to deal with the child or a child's parent over data protection issues.

Requests to view or receive copies of records should be made in writing to head teachers and then 15 school days are allowed in which the school should respond. If asked to provide a hard copy of the record, a fee may be charged according to the number of pages (see scale below).

Students may be asked for information to verify their identity, such as former pupils who may not be known to the school. They may also be asked for information to enable the school to locate the data held about them. For instance a student may be asked to supply the dates between which he or she attended the school.

In addition to the subject access right which can be exercised by pupils or by parents acting on behalf of pupils, parents have their own independent right of access to the official educational records of their children under separate education regulations.

If the data subject, parent or pupil is treated in a manner which is decent, legal, honest and truthful their data protection rights will almost certainly be protected and the school will be well on the way to meeting their obligations under the DP Act 1998.

Subject Access Fees

No of Pages	Maximum Fee	No of Pages	Maximum Fee
1-19	£1	100-149	£10
20-29	£2	150-199	£15
30-39	£3	200-249	£20
40-49	£4	250-299	£25
50-59	£5	300-349	£30
60-69	£6	350-399	£35
70-79	£7	400-449	£40
80-89	£8	500+	£50
90-99	£9		

.....

There is a dedicated page relating to Data Protection and Freedom of Information available on ClusterWeb under Services & Guidance together with a section under Forums (there is also a quick link in top right hand corner of home page). This is where you can locate the Records Management Toolkit together with the Retention Schedule for Schools http://www.clusterweb.org.uk/cwpages/Services/dpfoi.cfm

For further guidance/advice relating to Data Protection please contact:

Michelle Hunt
Freedom of Information & Data Protection Co-ordinator
Children, Families & Education Directorate
Room 2.35 Sessions House
Tel: 01622 696692
Email: michelle.hunt@kent.gov.uk.