Human Resource Service

Data Protection

Guidance

A model for Schools

Essex County Council

Data Protection Procedure
A Model for Schools

Published by:
Essex County Council HR Service
County Hall, Chelmsford
Essex CM2 6WN
England

©Essex County Council HR Service 2003 issued October 2003

CONTENTS **PAGE NO:**

1 Introduction 3
2 The Data Protection Act 1998 3
3 Notification 3
4 Principles of Data Protection 4
4.1 Principle 1: Personal data will be processed fairly and lawfully. 4
4.2 Principle 2: Personal data will be obtained only for one or more specified and lawful purposes. 5
4.3 Principle 3: Data must be adequate, relevant and not excessive. 5
4.4 Principle 4: Data must be accurate and up to date 5
4.5 Principle 5: Data must not be kept for longer than required for the purpose. 5
4.6 Principle 6: Data must be processed in line with individual's rights. 6
4.7 Principle 7: Data must be processed in a secure manner 7
4.8 Principle 8: Data shall not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection 7
5 Responsibilities under Act 8
5.1 Governing Body 8
5.2 Headteacher 8
5.3 Data Controller 8
5.4 All Staff 8
6 Access to Information 9
7 Dealing with Access Requests 10
8 Disclosure of Data 10
8.1 Staff who need to know 10
8.2 Purposes specified 10
8.3 Specific agreement of data subject 10
8.4 Telephone enquiries 11
8.5 Police 11
8.6 Third Party Disclosures 11
9 General Guidance for staff 12
9.1 Recruitment and Selection 12
9.2 CRB checks (SD2 forms) 13
9.3 Confidential References 13
9.4 Education Records 14
9.5 Examination Results 14
9.6 Home Addresses and Telephone Numbers 15
9.7 E-mail Addresses 15
9.8 Sickness and Accident Records 15
9.9 Pension and Insurance Schemes 16
9.10 Photographs, Videos and CCTV 16
9.11 Equal Opportunities Monitoring 17
9.12 Discipline, Grievance and Dismissal 17
9.13 The Internet 18
9.14 Collecting Personal Information 18
APPENDIX 1 19
APPENDIX 2 21
APPENDIX 3 23
APPENDIX 4 25

1 Introduction

This document sets out the school's responsibilities under the Data Protection Act 1998 and provides guidance on the maintenance of and access to employment and educational records in accordance with the provisions of the Act.

2 The Data Protection Act 1998

The Data Protection Act 1998 received Royal Assent on July 16th 1998 and came into force on 1st March 2000. It introduced into UK law the provisions of the European Commission Data Protection Directive (95/46/EC). The 1998 Act strengthens and extends the Data Protection regime created by the 1984 Act. It applies to anyone who processes, stores or is the subject of personal data.

The Act works in two ways, it says:

- Anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow the eight principles of 'good information handling' (see section 4).
- All individuals (data subjects) have the right to see information that is held about them and the right to have information corrected if it is wrong.

The 1998 Act covers all electronic records and extends data protection to manual files where the data on a data subject is readily accessible (a structured filing system). Manual files opened on or after 24 October 1998 for any new purpose (as defined in the Act) come under the new Act, whereas files for existing before that date will not be fully covered until 2007, though subject access requests were possible from 24 October 2001.

The main aim of the 1998 Data Protection Act is to protect data from unwanted or harmful uses and to provide an individual with some control over the use of their personal data.

3 Notification

Notification replaces what used to be registration under the 1984 Act, and is the process by which the data controller's details are added to a public register. This register is maintained by the Information Commissioner and can be consulted by individuals to find out what processing of personal data is being carried out by a particular data controller. The school, or governing body as data controller, is required to ensure its entry in the register is up-to-date. Failure to comply is an offence.

The information that will be required for notification includes:

- Name and address of data controller.
- Nominated representative (if applicable).
- Description of the personal data being processed and the category of data subject to which they relate.
- Description of the purpose(s) for which the data is/are being processed.
- Description of any recipients to whom the data will be disclosed.
- Names of any countries outside the EEA to which data is or will be transferred.

4 Principles of Data Protection

In collecting and using data the school will comply with the requirements of the Data Protection Act that govern the processing of personal data. Under these requirements, the information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The school and its staff who process or use personal information will ensure they comply with the following 8 principles of good practice which are laid out in the Act:

4.1 Principle 1: Personal data will be processed fairly and lawfully.

The collection and disclosure of data is subject to scrutiny and is only 'lawful' if it meets at least one of the following criteria (as specified in Schedule 2 of the Act):

- With the consent of the data subject, or,
- In performance of a contract (for example to process an application as part of the admissions process), or,
- If there is a legal obligation (for example under prevention of terrorism legislation), or
- For the protection of the vital interests of the individual (for example to prevent injury or other damage to the health of the data subject), or,
- In the legitimate interest of the data controller, unless it is prejudicial to the interests of the individual (for example for the purpose of equal opportunities monitoring).

(For a full definition of 'processing' see Appendix 3).

Personal Data must meet all of the following criteria in order to be processed 'fairly':

- Data will only be collected from persons who have the authority to disclose it. If personal information is collected from a third party, the data subject will be informed of the 'use' of the information.
- Subjects will not be deceived or misled in any matter related to the use of personal data.

In addition to the requirements outlined above, Sensitive Personal Data may only be processed if it also meets at least one of the following criteria (as specified in Schedule 3 of the Act):

- The Data Subject has given explicit consent.
- It is necessary to meet requirements of employment law.
- It is necessary to protect the vital interests (i.e. if the situation is a matter of life or death) of the subject or another person.
- The data subject has already manifestly made the information public.
- It is necessary for legal proceedings, obtaining legal advice or defending legal rights.
- It is necessary for the carrying out of official or statutory functions.
- It is necessary for medical purposes.
- It is necessary for equal opportunities.
- It is necessary in order to comply with legislation from the Secretary of State.

For a full definition of Sensitive Personal Data see Appendix 3.

4.2 Principle 2: Personal data will be obtained only for one or more specified and lawful purposes.

Data will not be further processed in any manner incompatible with the initial specified purpose or those purposes for which it was obtained. To satisfy the first principle (fair processing) the data subject(s) must not have been misled or deceived as to the reason(s) for processing.

4.3 Principle 3: Data must be adequate, relevant and not excessive.

Personal information, which is not necessary for the intended processing, must not be acquired i.e. personal information cannot be collected just because ‘it may be useful’.

4.4 Principle 4: Data must be accurate and up to date

The school must ensure that there is a system in place to review data for accuracy and to ensure that it is up to date. Procedures must be in place to make any amendments requested by a data subject, or a record kept if the amendment is not considered appropriate.

4.5 Principle 5: Data must not be kept for longer than required for the purpose.

The school must indicate the length of time that data is to be in use and archived for any given purpose. This time period must be seen as justifiable for the particular purpose and in line with any legislation covering the processing.

Information should not be kept any longer than the time period indicated to the data subject. The school must regularly review data held in order to assess whether information is still required.
The Act recommends the school to have a retention policy in place to ensure information is retained only for as long as is necessary. Appendix 1 illustrates for guidance purposes the length of time records must be retained for legal reasons.

The Data Protection Act recommends the school to have a disposal policy in place to which all staff can refer when they need to dispose of personal information. A disposal record will assist the school in responding to enquiries made under the Data Protection Act. Before disposing of any data the school will consider the following key points:

- Any legal requirements (e.g. possible negligence action).
- The length of any appeals procedure relating to the information.
- The number of times in the last two or three years that a particular type of record has been accessed.

4.6 Principle 6: Data must be processed in line with individual's rights.

This is strongly linked to the first principle of fair and lawful processing. Data subjects have the right to know details of the processing and the right of access to personal information.

A data subject (including a member of staff) has the right to object to data processing relating to them which is likely to cause substantial and unwarranted damage or distress to that data subject or another person. There are a number of provisos to this right, in particular:

- The damage or distress must result from unwarranted processing, or
- The data subject must not have given consent to the processing, or
- The processing is not necessary for the purposes of fulfilling a contract with the data subject; or for fulfilling a legal obligation of the school, or for protecting the data subject’s vital interests.

In addition the Act gives data subjects the right to object to processing used for the purpose of direct marketing and/or wholly automated decision making.

Data subjects have the right to rectify inaccurate data and to block future processing in cases of unlawful/unfair processing. Data Subjects must formally request their rights in writing and their rights are enforceable by the courts.

4.7 Principle 7: Data must be processed in a secure manner

The school must guard against unauthorised and unlawful processing (e.g. access, alteration, disclosure or disposal). Appropriate security records must be kept in order to provide an audit trail. Personal information will, so far as possible, be

- Kept in a locked filing cabinet, or
- In a locked drawer; or
- If it is computerised, be password protected, or
- Kept only on disk which itself is kept securely.

When personal data is to be destroyed, paper or microfilm records will be disposed of by shredding or incineration; computer hard disks or floppy disks will be re-formatted, over-written or degaussed.

4.8 Principle 8: Data shall not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection

If the Data is to be transferred to a country or territory that does not have adequate protection then at least one of the following conditions must be met:

- The Data Subject has given consent.
- It is necessary for the performance of a contract with the Data Subject.
- It is necessary for the performance of a contract that is in the interests of the Data Subject.
- The transfer is necessary for reasons of substantial public interest.
- The personal data is already on a public register.
- The transfer is necessary to pursue legal proceedings, legal advice or defending legal rights.
- It is in the vital interests of the data subject
- The Information Commissioner has approved the transfer on the grounds that it safeguards the rights and freedoms of the Data Subject.

5 Responsibilities under Act

All staff have a duty to observe the principles of the Act. (See section 4 page 5). These guidelines are intended to assist staff to understand the aims and principles of the Act and to set out the main areas in which staff are likely to be affected by data protection issues in the course of their work.

5.1 Governing Body

The Governing Body has responsibility for:

- Ensuring the implementation of the Data Protection Act.
- Ensuring that school policies, procedures and practice are consistent with the objectives of the policy.
- Ensuring that complaints are investigated and dealt with effectively.
- Ensuring that appropriate training takes place for the Headteacher and all staff.

5.2 Headteacher

The Headteacher is responsible for:

- Ensuring that the Data Protection policy is implemented in the schools procedures and practices.
- Ensuring that the procedure is brought to the attention of all employees and that all staff receive appropriate training.
- Compliance with the procedure at a practical level through action in recruitment and selection, training and development and general management.
- Encouraging good practice by all staff and dealing appropriately with breaches of the Act.

5.3 Data Controller

The Governing Body is the school's Data Controller. Where the Governing Body considers it appropriate a designated person may be nominated to act as Data Protection Officer to help ensure compliance within the school. The Data Controller is responsible for:

- Implementing and monitoring staff and other data subjects when processing data.
- Providing advice on the aspects of data protection.
- Determining the purposes for which and the manner in which any personal data is, or is to be, processed.

5.4 All Staff

Staff must ensure they understand how their work is affected by the Data Protection Act and abide by the principles of the Act. All staff must assess the information used in the course of their work and their responsibility for

any personal data. Failure to abide by the requirements of the Act is a criminal offence and an individual may be held personally responsible for any non-compliance.

It is a condition of employment that employees will abide by the rules and policies made by the school from time to time. All staff must be aware of and ensure that they comply with this procedure.

If there are any questions regarding the Data Protection Act and its implications please contact ……(School Governor or nominated data protection officer).

6 Access to Information

The Data Protection Act gives all individuals about whom the school holds personal information the right to access information that relates to them whether it is held electronically or in manual form. Although the Act refers to a structured manual filing system, access to information held in an unstructured filing system may also be requested but further information may be required from the data subject to help the school retrieve the data.

The school will only allow access once a request has been received in writing (or email) and the school is satisfied as to the identity of the person making the request. Proof of identity, confirming name and address, will be requested for this purpose. Only a child's parent or legal guardian may make requests for access to their child's educational records. Proof of this relationship will be required before access is granted.

On request the school will inform the data subject of:

- The personal data of which that individual is the data subject,
- The purpose or purposes for which the information is or are to be processed, and
- The recipients or classes of recipients to whom the information may be disclosed.

Once a request has been received, the school will grant access to the data held but will not allow any information to be copied or taken away by the data subject. The data subject is however entitled to request a copy of the information related to them which will be supplied by the school unless the supply is not possible or would involve disproportionate effort.

The right of access extends to children and young people under 18 who understand what it means to exercise that right. Where a child or young person under 18 makes a request for access to their records, the school or a relevant authority (e.g. doctor or educational psychologist) will decide whether or not he/she has sufficient understanding to do so.

7 Dealing with Access Requests

The school will comply with requests for access to personal information as quickly as possible and will ensure that requests for access are dealt with within the timescale specified by legislation.

Request for access made by students and parents will be dealt with within 15 school days. The school will process requests from all other data subjects within 40 days. An initial response will be sent to the requestor within twenty-one days of receiving an access request. The response will confirm the request has been complied with, indicate the intention to comply, or give the reasons for regarding the request as unjustified.

If, for any reason, these timescales cannot be met, the reason will be explained in writing to the individual making the request.

Any person wishing to exercise their right of access should obtain a copy of the school's access to information form (see Appendix 2 for sample form).

8 Disclosure of Data

The following attempts to illustrate when data can be disclosed. This list is not exhaustive.

8.1 Staff who need to know

Data will be disclosed to members of staff who need to know it in order to carry out their normal duties. However, only that data required will be disclosed.

8.2 Purposes specified

Data will only be disclosed for use within the purposes originally specified when it was collected. Any other use amounts to unlawful processing. For example, if information is collected in order to pay school uniform grants in 2002 the school will not be allowed to use that information as a mailing list for a library service.

8.3 Specific agreement of data subject

Data will be disclosed to a third party if the data subject has given specific consent, ideally in writing. In such cases, consent will be obtained prior to the disclosure.

8.4 Telephone enquiries

Requests from third parties are often made by telephone, with the added problem of verifying the identity of the caller. Even when the call appears to be genuine, data will not be disclosed. Instead, an offer will be made to contact the data subject concerned, on behalf of the caller, or to pass on a message.

8.5 Police

Disclosures to the Police are not compulsory except in cases where the school is served with a Court Order requiring information. Requests from the police for access to information must be made in writing. In cases where the school has not been served with a Court Order but receives a request, consideration must be given to the implications of disclosure before any action is taken. The school may be required to provide explanation for any disclosure of the data subject's personal information at a later date and must be able to provide justifiable reasons for doing so e.g. where the school believes that failure to release the information would prejudice an investigation.

8.6 Third Party Disclosures

There are a number of circumstances under which data can be disclosed to a third party without the consent of the data subject.

The circumstances are set out in the Act as follows:

- Data required by law – for example data supplied to statutory bodies.
- Data that is in the vital interests of the data subject – for example in a life or death situation.
- Data that would prevent harm to a third party.
- Data that would prevent a crime.
- Data that would be in the interests of national security.

Even in these circumstances, proof of identity, confirming name and address and a request in writing, will be required where practicable. Where the information requested is that of a pupil the requestor must also provide evidence of their relationship to the child. Access requests to educational records may only be made by the child's parent/legal guardian.

9 General Guidance for staff

The school needs to collect and use data (information) for a variety of purposes about its staff and other individuals who come into contact with the school. The purposes of processing data include the recruitment and payment of staff, organisation and administration of courses, monitoring of health and safety arrangements, monitoring of performance and achievements and compliance with statutory obligations of the LEA, government agencies and other bodies.

Included below is a list of general areas where the issue of data protection may arise. These guidelines do not attempt to cover every situation.

9.1 Recruitment and Selection

It is important to ensure that applicants who are responding to job advertisements or completing application forms know exactly to whom or where they are supplying their information and for what their information will be used. Only information relevant to the recruitment decision should be requested. Applicants should have explained to them as early as possible what verification checks may be undertaken. This is currently covered in the application form where the individual is requested to sign a declaration of consent.

Before attempting to obtain any information from a third party, for example for the purpose of confirming qualifications or employment history, it is necessary to obtain a signed consent form or some similar form of consent from applicants (this is currently covered in the declaration of consent on the application form). Information should not be sought from applicants unless it can be justified as being necessary to enable the recruitment decision to be made, or for a related purpose such as equal opportunities monitoring. For example, there is no obvious reason why the school should ask applicants for information about their membership of a trade union.

It is important to ensure that personal data used during, and retained after the interview process, is justifiable against any challenge of it being relevant and necessary. The school may be asked to prove that the non-selection of a candidate was on the basis of something other than a discriminatory attitude held by the interviewer. Applicants will have subject access rights regarding interview notes taken. It is for this reason that all interview notes must be legible and understandable. It is recommended that interview notes be kept for a period of 6 months after the date of interview.

9.2 CRB checks (SD2 forms)

The school will require all short-listed applicants for all posts to declare criminal convictions, which are 'spent' or 'unspent' and including any cautions, and pending prosecutions. Such declarations will be made on the relevant self-declaration form (SD2) and will be submitted, in a sealed envelope, marked private and confidential, to the Chair of the selection panel or nominated Human Resource Officer, prior to interview. This information must only be disclosed to those that are authorised to see it in the course of their duties.

Information received via a Form SD2 'disclosure of criminal convictions (spent and unspent)' or a 'CRB disclosure application form' must be treated as strictly confidential and only considered in relation to the post being applied for.

Once a recruitment (or other relevant) decision has been made, disclosure information should not be kept for any longer than is absolutely necessary. For those applicants who are not appointed this should generally be for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. Once the retention period has elapsed, the school must ensure that any disclosure information is destroyed by secure means, e.g. by shredding.

Once the CRB process has been completed, the SD2 form should be destroyed for both the successful and unsuccessful candidates.

9.3 Confidential References

The Data Protection Act allows data subjects to access references about themselves *received* by the school (subject to respecting the confidentiality of third parties), but not those *provided* by the school.

Although confidential references received by the school are not exempt from the right of access, consideration must be given to the data privacy rights of the referee. Information contained in, or about, a confidential reference need not be provided in response to a subject access request if the release of this information would identify an individual referee unless:

- The identity of the referee can be protected by anonymising the information,
- The referee has given his/her consent, or
- It is reasonable in all the circumstances to release the information without consent.

The school may not refuse to disclose references received from third parties without providing reasons e.g. the referee may have refused permission for the information to be made available, or the disclosure may result in harm to the referee.

In cases where a confidential reference discloses the identity of an organisation, but not an identifiable individual, as referee, disclosure will not breach data privacy rights.

Confidential references written by the school are exempt from subject access requests. However, the school is recommended to adopt an open reference policy whereby the information contained within a reference is shared with the data subject on request. This helps alleviate any cause for concern by the data subject at a later date.

When writing a reference it must be kept in mind that the details of the reference may, at a later date, be disclosed to the individual (for example by the new employer). The school must ensure that all information provided is up to date and accurate.

Where a reference requests it, the school can disclose information regarding the number of day's sickness of a data subject. However, detailed information about the data subject's health or sickness record (including reasons for absence), falls within the definition of 'sensitive personal data' and must only be disclosed with the explicit (i.e. written) consent of the data subject.

9.4 Education Records

The 1998 Act sets out specific rights of access for school pupils to their educational records. Educational records are the official records for which Headteachers are responsible. All current and former school pupils, regardless of age, have a right of access to their official educational records held within the school. While in principle students have a right of access to the whole of their educational records, in exceptional cases some information may be withheld. The main exemptions are for information which might cause harm to the physical or mental health of the student or a third party, information which may identify third parties (for example other pupils), and information which forms part of some court reports. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.

9.5 Examination Results

The school must ensure that strict confidentiality and secure office practices are followed while papers are being marked and while results are being compiled. The Act does not give pupils the right to access their own examination scripts but it does allow access to comments made upon them by examiners. However, pupils are able (under subject access rights) to see the breakdown of marks awarded for particular questions, or sections of examinations.

Examination marks should not be shared (either verbally or in writing) with any other person unless the individual pupil has given their permission e.g.

the displaying of examination results on a school notice board, or a list sent around the classroom is prohibited.

9.6 Home Addresses and Telephone Numbers

Home addresses or telephone numbers of staff or other data subjects must not be given out to third parties unless the individual has given permission to do so.

Alternative approaches include taking the caller's contact details and advising that a message will be passed on requesting that the caller is contacted, or offering to forward correspondence to a pupil or a member of staff on behalf of the caller.

It is important to take care when handling such requests. An individual's pupil/staff status is personal data. The school should be careful to neither confirm nor deny that the person is a pupil or member of staff at the school, or that the person is otherwise known to the school.

9.7 E-mail Addresses

Personal and/or work email addresses must not be disclosed. If asked to disclose another member of staff's personal email address, the caller can be asked to give their email address and told that it will be passed on to the individual they are trying to contact ‘if’ they are a member of the school. It is not appropriate to disclose a colleague's work details to someone who claim they wish to contact them regarding a non-work related matter.

9.8 Sickness and Accident Records

Sickness and accident records will include information about an employee’s physical or mental health. These types of record should be treated as sensitive personal data and are therefore subject to specific extra requirements under the Act (see section 4, page 6).

The Act makes a distinction between sickness, accident and absence records. Sickness and accident records contain details of the illness, condition or accident suffered by the individual. Absence records however, may explain the reason for the absence as ‘sickness’ or ‘accident’ but do not include any reference to specific medical conditions. The information commissioner recommends that sickness and accident records should be separated from absence records and that sickness and accident records should not be accessed where records of absence could be used instead.

In order to hold these records, the school has to satisfy at least *one* of the conditions for processing sensitive personal data,

Those conditions that may be most directly relevant to sickness and accident records are:

- The processing is necessary for the purposes of the exercising or performing of any right or obligation, which is conferred or imposed by law on the school in connection with employment. This could include obligations under health and safety legislation or for the purpose of administering statutory sick pay. This condition may also be relevant to the need to maintain sickness records so that the school can ensure that an employee is not dismissed on sickness grounds, when it would have been unfair to do so.

- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. This condition may therefore apply where the school is defending itself against tribunal or court proceedings.

- The data subject has given his or her explicit consent to the processing. This will only apply where the employee understands what personal data is involved and has given a positive indication of agreement (such as a signature). The consent must also be freely given and not made subject to a detriment if the employee withholds their consent.

Being known as an employee of the school may mean being asked for information, for instance by parents about a member of staff who is off sick. Although this can be awkward, parents must be informed that employees are unable to discuss confidential school matters. Persistent enquiries must be referred to the Headteacher.

9.9 Pension and Insurance Schemes

Pension schemes, private medical and permanent health insurance schemes are typically administered by schools (or LEA) but provided or controlled by third parties. Data required to administer such schemes should not be used for other purposes and any data passed to the scheme providers should be limited to that which is necessary to operate the relevant scheme. It should be made clear to employees who join these schemes what data will be passed between the employer and the scheme controller and for what purposes this will be used.

9.10 Photographs, Videos and CCTV

Where it is wished to take photographs or make video recordings of staff and/or pupils, as individuals, as small groups or organised groups, the individual(s) concerned must give their consent and be informed of the purpose(s) for which the information is to be used. For general photographs or video recordings of the school grounds and public places, whereby individuals can not be identified, consent is not required. If the school intends to record a school event such as a sports day or school play, parents must be informed of the intention and the purpose(s) for

which the recording will be used. A parent may chose to withdraw their child from such an event if they object to the recording.

The school must ensure the recorded images are stored securely, where only a limited number of authorised persons have access to them. The recorded images must only be retained long enough for any incident to come to light (e.g. for a theft to be noticed). The school may disclose recordings to a law enforcement agency in order to help with the prevention or detection of crime (see section 8.5) but must not release the images to any other third party.

For further guidance on the use of CCTV please refer to the Information Commissioners website under 'codes of practice our response and other papers'. http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

9.11 Equal Opportunities Monitoring

The Act specifically allows for processing of data on racial or ethnic origin, religion and disability if it is necessary for keeping under review the existence, or absence, of equality of opportunity. The collection of this information is exclusively used for the statistical evaluation of the school's equal opportunities policy within recruitment and employment.

The school, where possible, will ensure anonymity of information when meaningful monitoring is required. The equal opportunities monitoring form, which collects information for this purpose, must be removed from all applications before any assessment of suitability for the post is considered.

9.12 Discipline, Grievance and Dismissal

Employees have the same rights of access to files containing information about disciplinary matters or grievances about themselves as they do to other personal data held, unless this information is associated with a criminal investigation, in which case an exemption might apply. All of the normal data protection and access obligations apply to data created or accessed in the course of dealing with disciplinary and grievance issues. Any information referring to a third party must be removed or anonymised before access is granted.

Disciplinary warnings typically 'expire' after one year provided that no further warnings have been issued and no disciplinary action has been taken against the employee during that period. In these circumstances, the warnings will generally be disregarded for future disciplinary purposes but not removed from the personal file. There may be occasions, however, for example in the case of gross misconduct, or gross negligence, where the nature of the offence does not make it desirable and practicable for the one year time limit to apply. If this is so, the employee must be notified in writing when the warning is given of the period applicable, which will not normally exceed 5 years. Exceptions to the time limit will apply where child protection issues are raised - refer to the Child Protection procedure for further information.

Details regarding information relating to discipline/grievance issues must not be disclosed to a third party. For example, being known as an employee of the school may mean being asked, for instance by parents, about the alleged suspension of another member of staff. Under no circumstances should this information be disclosed or confirmed and persistent enquiries must be referred to the Headteacher.

9.13 The Internet

Data placed on the school's web site and made available via the Internet will be available in countries which do not have a data privacy regime considered adequate by the EU. Where the school wishes to make staff/pupils personal data available in this way, the consent of the staff and/or student(s) concerned must be obtained. Consent can be withdrawn at any point.

Internet pages are sometimes used to collect personal data such as names and addresses of individuals who request school information e.g. from those who are registering to attend an open day. The relevant web page should indicate the purpose or purposes for which the data is collected, the recipients to whom it may be disclosed and an indication of the time period for which it will be kept (e.g. "while we process your application", rather than a specific date).

All sites that collect information from site visitors must provide a Privacy Statement. The purpose of this statement is to help individuals to decide whether they want to visit the site and, if so, whether to provide any personal information. Privacy Statements must be prominently displayed. The following is an example of a privacy statement:

> "This Website aims to provide on-line information about all of the schools services. We do not use cookies for collecting user information from the site and we will not collect any information about you via this website without your consent".

Individuals must be given the opportunity to opt out of parts of the collection or use of the data not directly relevant to the specific purpose.

9.14 Collecting Personal Information

Before collecting or processing personal information the school must consider whether the information collected on staff and other data subjects is necessary for the employment relationship. For example, information concerning an employee's life outside work is unlikely to be necessary. However, it might be legitimate to request information about an employee's other jobs where there is a justifiable need, for example, in connection with Working Time Regulations, or to request information about their children in connection with an application for parental leave.

APPENDIX 1

The following table illustrates, for guidance purposes, the length of time records need to be kept for legal reasons (This is not an exhaustive list. Medical records are kept for a variety of health and safety reasons and will carry various retention times).

Type of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings	7 years from the end of employment	References and potential litigation
Staff application forms/interview notes	At least 6 months from the date of the interview	Time limits on litigation
Facts relating to fewer than 20 redundancies	3 years from date of redundancy	As above
Facts relating to 20 + redundancies	12 years from date of redundancy	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax [Employment] Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay [General] Regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay [General] Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books; records and reports of injuries and diseases	At least 3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1995
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress-related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	COSHH Regulations 1999

Ionising Radiation Records	At least 50 years after last entry	Ionising Radiation's Regulations 1985
Education records, including academic achievements and conduct	At least 6 years from the date the student leaves, in case of litigation for negligence	Limitation period for negligence

APPENDIX 2

…….....……..... .. (School Name)

DATA PROTECTION ACT 1998 - DATA SUBJECT ACCESS REQUEST FORM

Under section 7 of the Data Protection Act 1998, an individual is entitled to ask for information the school holds about her/him. This entitlement is known as the "Right of Access to Personal Data."

In exercise of the rights granted to me under the Data Protection Act 1998, I request that the …….***(school name)*** provides me with details of the personal data it holds about me and the purposes for which it is used.

I am aware that, under section 7.3 of Data Protection Act 1998, the school is not obliged to comply with my request unless they are supplied with such information as they may reasonably require in order to satisfy themselves as to my identity and to locate the information which I seek.

DATA SUBJECT (please use BLOCK CAPITALS)

Full Name……Date of birth…….
Address
……...
...……Post code…….
Telephone no…….... Length of time at this address ……yrs……mnths
Previous address(es) with dates (if data is required for this period)
……
……

Declaration – please complete section (a) and either section (b) or (c)

Section (a) (please tick)

I am providing proof of identity through:

- ❑ my driving licence
- ❑ passport
- ❑ birth or marriage certificate
- ❑ benefit book

and confirmation of my current permanent home address is provided through:

- ❑ the same document
- ❑ a current utility bill in the same name as my birth/marriage certificate

And either section (b) I confirm that I am the Data Subject.

Signed…….
Date……..

Page 1 of 2

Or section (c) I confirm that that I am acting on behalf of the data subject and have submitted proof of my authority to do so.

Signed……..
Date…….

Full Name……Date of birth……..……
Address…….
……...……Post code……
Tel no……...

INFORMATION REQUESTED

Please complete the section below to enable the school to locate the information that you require.

INFORMATION REQUESTED (please use BLOCK CAPITALS, provide as much detail as possible and continue on separate sheet if necessary)

If you would like to provide us with other information on the data you are seeking, please use this space. If you want information that relates to a specific time period or experience, the details would help us to focus our search and respond more quickly.

……..……
……
……..……
……..……
……
……
……
……
……
……
……
……
……
……
……
……

Please return completed form with proof of identity and address to the Headteacher

APPENDIX 3

Key Definitions

Data Controller	The School/Governing Body will normally be the data controller. A 'data controller' is any person/authority who makes decisions with regard to particular personal data, including decisions about the purposes for which the data is to be processed and the way in which that processing takes place.
Data Subject	A ‘data subject’ is any living person who is the subject of personal data.
Data Subject Access	This is the right of an individual to see personal data relating to him or her that is held by a data controller.
Processing	This term covers almost any conceivable use of data, including obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying the information or data. This means, for example, that simply possessing data constitutes processing for the purposes of the 1998 Act. Some examples of processing: Filing, copying a disk, typing an email, deleting an email, archiving files, accessing details from a file, transcribing the contents of a tape, moving a filing cabinet that is full of files, shredding a file, using a camcorder, making a voice recording, keeping a list of contact names and addresses in a diary, keeping ad-hoc information about members of staff.
Structured Manual Filing System	This means any structured set of information which is organised either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual can be easily found.
Manual Records	The 1998 Act extends the definition of ‘data’ from that held in computer-based systems to include all information recorded manually as part of a ‘relevant filing system’. It is important to remember that guidance from the Information Commissioner indicates that this definition will be interpreted broadly.

Data	'Data' means information which, • Is being processed by means of equipment operating automatically in response to instructions given for that purpose, • Is recorded with the intention that it should be processed by means of such equipment, • Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or • Does not fall into any of the above catagories but forms part of an accessible record.
Personal Data	Personal data means data which relate to a living individual who can be identified from that information.
Non Sensitive Data	General personal details, such as name and address. Details about class attendance, marks and/or grades and associated comments. Reports and references. Notes of personal supervision, including matters about behaviour and discipline.
Sensitive Personal Data	Personal data consisting of information as to a person's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life or the commission or alleged commission of any offence (or proceedings for those offences) by that person. Examples of when sensitive personal data may need to be recorded include: the recording information about dietary needs, for religious or health reasons prior to taking students on a field trip, recording information that a staff member is pregnant, as part of pastoral duties or equal opportunity monitoring forms as part of the application process.

APPENDIX 4

The Legislative Framework for Data Protection

All staff also need be aware of their rights in relation to personal data held about them, how it is managed and how to request access to it. The Data Protection Act is about human rights, and specifically the right to privacy. The Data Protection Act 1998, Human Rights Act 1998 and the Freedom of Information 2000 legislation are inter-linked. They are intended to help maintain a fair balance between the rights and interests of individuals, in particular between the freedom to process information on the one hand and rights of privacy on the other.

In order to fully integrate and understand the key objectives of the Data Protection Act it is important to have an awareness of the legislative framework. A summary of the related legislation can be found below.

The Human Rights Act 1998

The Human Rights Act came fully into effect on 2 October 2000. It gives further effect in the UK to the fundamental rights and freedoms guaranteed under the European Convention on Human Rights. The Act states that everyone has 'the right to respect for his private and family life, his home and his correspondence'. No interference by a public authority is permitted unless it is 'in accordance with the law'. Any law legitimising interference must be 'necessary' in a democratic society e.g. national security, crime, public health.

The principles of Data Protection are echoed in Article 8 of the European Convention on Human Rights. The Data Protection Act reflects the human right to privacy, for example by specifying criteria for CCTV usage and by requesting consent from data subjects before their personal information is used for any specified purpose.

The Freedom of Information Act 2000

The FOI Act (section 68) amends the Data Protection Act 1998 to bring under the provisions of the Act as personal data manual data, which is not part of a relevant filing system.

The Freedom of Information Act 2000 (FOI) provides the right to access a wide range of information held by public authorities. In conjunction with the Data Protection Act, the two regimes provide a comprehensive framework of access rights across the full range of personal and non-personal information held by public authorities.

The Freedom of Information Act and the Data Protection Act operate in tandem under the supervision of the Information Commissioner. Once the

Freedom of Information Act is fully in force (1st January 2005), requests for access to personal information will be dealt with under the provisions of the 1998 Act and requests for access to other sorts of information will be dealt with under the Freedom of Information Act 2000

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 establishes a new legal framework to govern the interception of communications. It sets the rules regarding activities such as recording, monitoring or diverting communications in the course of their transmission over a public or private telecoms system.

The Act establishes the circumstances in which it is lawful to intercept communications. It authorises interception in cases where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented. It also provides for the Secretary of State to make "Lawful Business Practice" Regulations setting out the circumstances in which businesses can lawfully intercept communications without consent. The Lawful Business Practice Regulations will allow businesses to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the operation of their telecoms systems. Businesses will not need to gain consent before intercepting for these purposes although they will need to inform their staff that interceptions may take place.

The Data Protection Act 1998 and Regulation of Investigatory Powers Act 2000 work alongside side each other to ensure use of communications data is properly controlled and regulated with independent oversight and a proper complaints procedure.

Telecommunications (Lawful Business Practise) (Interception of communications) Regulations 2000

This Act empowered the Secretary of State to make regulations, which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the Regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place.

Lawful Business Practice Regulations (LBP)

The LBP Regulations authorise employers to monitor or record communications without consent for a number of purposes, including the following:

- To establish the existence of facts relevant to the business.
- To ascertain compliance with the regulatory or self regulatory practices or procedures relevant to the business.
- To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.
- To prevent or detect crime.
- To investigate or detect the unauthorised use of telecommunication systems.

The Regulations cover all types of communications including those that are Internet based, by fax and by email.

For further information, additional copies of this document or to pass on your comments, please contact:

By telephone:
Michelle Ward
HR Officer, Schools HR Advisory Team on
01245 436837 or ednet 30837

By email:
michelle.ward@essexcc.gov.uk

By post:
Essex County Council
Human Resource Service
HR Schools Team
County Hall, Chelmsford CM2 6WN

Essex County Council – making Essex a better place to live and work

The information contained in this leaflet can be made available in alternative formats: large print, Braille, audio tape or disk. We can also translate the information into languages Please call 01245 434090

printed by CDS

INVESTOR IN PEOPLE

POSITIVE ABOUT DISABLED PEOPLE

Printed on 75% recycled paper.