Lambeth Schools Data Protection guidance manual

Contents

1 Introduction

1. This guidance document sets out the how Lambeth Schools should handle subject access requests from individuals in line with the provisions of the Data Protection Act 1998 (DPA).

1.1 The right of access to personal data

1. The DPA provides individuals with a right to request access to the personal data that an organisation holds on them; this is called "the right of subject access". This right was introduced in order to promote the principles of transparency and accountability. It enables individuals to understand how their personal information is used, to check the accuracy of the information and exercise their rights over the processing of that information. The right of access to personal data can only be denied in limited circumstances, where one of the Act's exemptions apply.

1.2 What is a valid subject access request?

1. A valid request:

a) Must be for that individual's personal data;

b) Must be made in a permanent form (in writing, email/fax etc);

c) Should include the appropriate fee; and

d) Must contain sufficient information to verify the identity of the person making the request and to locate the information which that person seeks.

2. The request does not have to cite the DPA. Further, the Act is purpose blind; this means that applicants do not have to explain the reasons why they are making a request. Once these criteria are fulfilled, the individual can expect his personal data to be provided within 40 calendar days (subject access requests for education records must be responded to within 15 school days).

3. Where a person is unable to make a written request without support or because English is not the person's first language you should consider referring them to the Citizen Advice Bureau or Children's Rights Service.

1.3 What is "personal data"?

1. Personal data is information which relates to an individual and which can identify that individual, either on its own or when combined with other information held by the school (e.g. an e-mail about a pupil which does not mention names but does include a reference number that can be linked to a specific individual). In the case of Durant v Financial Services Authority (2003) this definition has been refined to indicate that, in order to be considered

personal data, the focus of the information in question must be on the individual. For example, the minutes of a meeting will not be personal data if the individual's name is simply mentioned in the list of attendees. However, if the meeting is in full or in part about the individual then that document (or the relevant part) is their personal data. Personal data can be simply a name and reference number; alternatively it could be an entire folder (e.g. a pupils records, school employee file).

2. Examples of personal data that schools hold include; Pupil records, emails between staff relating to a particular pupil, human resources files for staff at that school.

1.4 Who can make a request under the Act?

1. Any living individual has a right to request access to the personal data that a school holds on them. A pupil of the school, a school employee, a parent of a pupil, or any other person that your school holds personal data on will therefore have a right to request access to their personal data.

1.5 Making a request on behalf of another person

1. A data subject may authorise any other person (e.g. a relative) to make a subject access request on their behalf. In most cases written authority from the data subject should be provided before your school can comply with a request from an agent.

2. A child is, in theory, entitled to a make a subject access request. However, a request from a child should only be complied with if it is thought they understand the nature of the request. As a general rule, a child aged 12 or over is presumed to be of sufficient age and maturity to be able to make a request for their own data. Where a child is deemed able to make a subject access request, the person handling the request should reply directly to the child.

4. If the child is not of sufficient age and maturity, then a person with parental responsibility is entitled to make a request on their behalf. The officer should be satisfied that the person with parental responsibility is acting in the best interests of the child before releasing the data. Caution should be exercised where child custody or abuse cases are concerned and where the Child has given information to a teacher or a support staff officer on an expectation of confidentiality.

5. Parents have a separate right of access to their child's official educational record under the Education (Pupil Information) (England) Regulations 2005. When considering whether or not to disclose information to the parent consider the same exemptions that apply to subject access requests under the Data Protection Act (see section 3 for more information on the exemptions). Under the Regulations, requests from parents to view their child's educational record should be dealt with by the Board of Governors. All

other requests for personal information from the pupil, or someone acting on their behalf, should be dealt with by the school.

6. An agent appointed by the Court of Protection or with a valid Power of Attorney may make a request on behalf of a mentally incapacitated individual.

7. Upon receipt of such a request, the person dealing with the request should check the validity of the Power of Attorney or the Court of Protection Order. A Power of Attorney must specify the purposes for which it is granted and it must be a certified copy (i.e. the document has the original stamp and signature of a solicitor).

8. Take care with spouses, partners or other relatives who may claim to be authorised to access the data – unauthorised disclosures to family members are a frequent cause of complaint to the Information Commissioner.

1.6 What about rights of access to information relating to deceased individuals?

1. The DPA only applies to the personal data of living individuals and as such does not give rights of access to deceased individuals' data.

2. Whilst the DPA does not apply to deceased individuals' information, schools still owe a common law duty of confidentiality to the deceased person and legal advice should be sought before disclosing information relating to deceased individuals.

1.7 What is an individual entitled to following a subject access request?

1. Upon making a request in permanent form, and paying the £10 fee[1], an individual is entitled to be told whether the school is processing that individual's personal data. If the School is, the individual is entitled to a description of:

a) The personal data;

b) The purposes for which they are being processed; and

c) Those to whom the data are or may be disclosed;

2. The individual is also entitled to a copy of the manual and computerised personal data the school holds on them (unless an exemption applies – see section 3). The personal data should also be provided in an intelligible form (see section 2.4.2).

[1] the fee is different if the request is for manually held education records – see section 2.1.4

3. The entitlement is to receive personal data not documents and as such an individual is not necessarily entitled to the original documents and all the information that they contain. However, providing copies of the documents that contain personal data is often the simplest and most cost effective way of dealing with a subject access request.

1.8 Does the DPA give an individual the right to view their personal data?

1. Individuals may request, or even demand, to view their file. The DPA does not provide individuals with this right. The Act only entitles them to copies of their personal data (i.e. through the provision of photocopied documents containing personal data). However, the Act provides that schools can fulfill their obligations under the subject access provisions by allowing an individual to view their records (rather than being provided with a copy), providing that the individual agrees to this proposal.

2. In the case of requests for particularly sensitive records it may be prudent to invite the individual into the school to view their records, with an appropriate member of staff available to help the applicant understand and “take in” the information that is held on them.

3. If an individual agrees to a viewing of their records and they have specific needs in relation to language or disability, arrangements should be made to present the information in a suitable manner and to involve approved interpreters. Consideration should also be given as to the accessibility of the building where the viewing is to take place.

2.0 Handling subject access requests

2.1 Clarifying the request, verifying identity, fee charging

2.1.1 Clarifying the request (section 7(3) DPA)

1. The Act allows schools to seek further information from the applicant, where this is reasonably required in order to be able to locate the information that the applicant is seeking access to.

2. General subject access requests for 'all personal data' are valid, and you should not simply ask the applicant to be more specific if the location of the data is already known. If clarity is sought please bear in mind that the applicant may not be aware of the different ways in which your school holds their personal data.

2.1.2 Verification of the identity of the individual (section 7(3) DPA)

1. Your school must be satisfied as to the identity of the individual making the request. This may be as simple as comparing the address and signature on held on file with the address and signature on their subject access request letter. However, if there is any doubt about the identity of the person making the request, further details should be sought.

2. Possible methods of checking identity in these circumstances include:

a) Asking the individual to give information which has been recorded as personal data by us and which the individual might be expected to know (for example the Universal Pupil Registration Number).

b) Asking the individual to produce a copy of a document that might reasonably be expected to be only in their possession (e.g. their birth certificate).

c) Asking the individual to have their signature witnessed by another person who is over the age of 18 and is not a relative (e.g. their Doctor confirms the individual's identity in a letter using the GP's headed paper).

3. If the request is from an agent of the data subject check that they have the necessary authority (see 1.5 above).

2.1.3 Charging a fee (section 7(2) (b) DPA)

1. Charging a fee for complying with subject access requests is discretionary. However, if your school is going to charge then the maximum is £10 in most cases (see 2.1.4 for other fee amounts).

2.1.4 Different fee for manual educational record requests

1. Where an individual (or their parent) requests access to the manual education records held on them by a school then Education Regulations permit that the school can charge a fee in line with the table set out in appendix 3. The maximum fee that can be charged in these circumstances is £50. However, this depends on the number of pages being photocopied.

2.2 Time limits (section 7(10) DPA)

1. The statutory time limit for complying with a subject access request is 40 calendar days (although, subject access requests for education records must be responded to within 15 school days). The 40 days will normally start from the date the school receives the request. However, if one or more of the items listed in (a) – (e) below have not been provided, the 40 day time limit will not commence until that item has been provided:

a) The fee.

b) Information reasonably required to validate the identity of the data subject.

c) Information reasonably required to locate the personal data requested.

d) Written authority from the data subject where another person is applying on their behalf.

e) A certified power of attorney or court of protection order (where applicable).

2. If the request does not meet the criteria identified in (a) – (e) a letter should be sent to the applicant/their agent requesting the necessary fee/information (The template letter in appendix 1 provides useful paragraphs for this purpose). Any further information/fee required should be asked for promptly; schools should not add their own delays to the process.

3. Confirmation of the fee having been processed should <u>not</u> hold up the process of dealing with a subject access requests. Once the fee (and other information) has been received the 40 calendar days start. If there is a problem processing the applicant's cheque then they should be notified as soon as possible.

4. One of the main reasons why people complain to the Information Commissioner is because their subject access request was not completed within the statutory time limit.

5. Every effort should be made to comply with the 40 calendar days time limit (or 15 school day time limit for education records). If it is clear that data collection and provision is going to exceed this limit, then the applicant should be advised of the date when their personal data is likely to be provided.

6. If you do not receive a response to the letter asking for the fee or the further information required, then you are not obliged to deal with the request.

2.3 Searching for records

2.3.1 Manual files

1. The type of manual files held on the data subject will depend on the nature of their involvement with your school. The computerized information held on an individual may well indicate if manual personal data is held.

2. Some manual files may be stored off site. It is important to confirm whether this is the case and ensure that these files are located so that access can be given.

2.3.2 Computerised personal data

1. School Management Information Systems holding data on:

(a) Pupils – personal, special needs and academic information

(b) Teaching staff – personal, payroll, Human Resources, contract and teacher work related information.

(c) Teaching and Special Needs support – contact details, payment, Human Resources and other specialist details

(d)Other staff – personal, payroll, Human Resources and contract information.

(e)Parents – contact details and other personal information

(f) Governors – contact details, responsibilities.

(g) Other contacts – service providers contact details

(h) Financial data – individual service providers for payment and invoicing

(I) Parent Teacher Association and other school fundraising organizations – contact details

(j) Other users of the school – organizations and individuals that use school premises, contact details

2.3.3 E-mails

1. You are also obliged to provide personal data held within e-mails. The Information Commissioner has developed guidance in this area as e-mail systems are often difficult to search. This guidance provides that it may be advisable to ask the data subject for additional information to help narrow down the search, and that the following should be taken into consideration:

a) Whether the data subject indicates that any data might be held in e-mails.

b) Whether the data subject can supply the authors and recipients of the e-mails.

c) Whether the data subject can indicate the subject of the e-mails.

d) Whether staff who have had dealings with the data subject are aware of e-mails exchanged either internally or externally relating to the data subject.

2. In the first instance, the person handling the request should contact those individuals who have had dealings with the data subject to see if there are any relevant e-mails in their email account (this is particularly relevant with regard to requests from employees and former employees of the schools). The e-mails containing personal data relating to the data subject should be copied and considered for disclosure against the Data Protection Act's exemptions. Further information should only be sought from the data subject where it is reasonably required in order to locate the data they are seeking access to.

3. It should be noted that it is a criminal offence for an individual to alter, block or destroy information, where their intention is to prevent the disclosure of the information to the data subject and no exemption from disclosure applies (see section 3).

2.3.4 CCTV

1. If your school uses CCTV cameras the images that they capture may need to be provided in response to a subject access request.

2. It is not necessary to check and supply footage unless the individual has specifically requested it. The following information will normally be needed from the applicant: date and place of the incident, approximate time, description of the individual e.g. what they were wearing, and any other information which may help identify the images requested.

3. If a request for CCTV footage is received and that information would normally be destroyed within the 40 calendar days for compliance with a request, then the footage must not be deleted until the data has been provided. Staff must not delete the recording solely on the basis that they want to prevent the data subject from gaining access, as this is a criminal offence.

2.3.6 Recorded telephone calls

1. An individual may request access to the personal data contained within a telephone recording and where the recording is held, this data can be provided in the form of a recording of the telephone conversation, or alternatively, through the provision of a transcript.

2. If the deletion date for the telephone recording occurs within the time period

for compliance with the request (40 calendar days), then the recording should not be deleted. Once you have given the individual a copy of it. You should confirm that the data has been/or is about to be deleted when providing your response (although it would be prudent to retain a copy if the information is likely to be needed later – e.g. in legal proceedings). Staff must not delete the recording solely on the basis that they want to prevent the data subject from gaining access, as this is a criminal offence.

2.3.7 Personal data held within unstructured manual records.

1. From 1 January 2005 individuals have had a right to request access to their personal data which is contained within unstructured manual records (i.e. in a manual file not held by reference to the individual).

2. If an individual is requesting access to personal data which is held within an unstructured record, they will need to specify the information that they are seeking so that it can be located (e.g. "I am requesting access to the personal data held about me which is contained in the minutes of your meeting of 5th June").

2.3.8 Schools Human Resources

1. The Schools Human Resources Unit based within the Council may hold information relevant to a request, where it is from an employee or former employee of the school and it would be worthwhile to check with the Unit, where the records held by the School suggest that the Schools Human Resources Unit have had involvement in the particular case.

2.4 Assessing the contents of a record (inc. third party details)

1. Once all the personal data requested has been located, the person handling the request should assess the content of the records for:

a) Third party data.

b) Unintelligible terms.

c) Personal data that is covered by one of the DPA's exemptions.

2. This section only deals with issues regarding third party data and unintelligible terms. Guidance on the Act's exemptions is contained in section 3.

3. If the information held is inaccurate then amendments should not be made before the data is sent to the individual. The individual should be informed that the school is aware of the inaccuracy and have taken steps to amend or annotate the original data.

2.4.1 Third party information (s.7(4) DPA)

1. The DPA acknowledges a third party's right to privacy where they can be identified from another individual's personal data (e.g. comments held on file which have been made by a child about their parent/carer). Section 7(4) of the Act introduces a number of criteria which aim to balance an individual's right of access against a third party's right to privacy. Personal data which also identifies a third party should be withheld unless:

a) The third party has consented to the disclosure.

b) It is reasonable in all the circumstances (see below) to comply with the request without their consent.

c) The third party identifiers can be removed from the document and the data subject can still receive the personal data contained within that document. In practice this may be difficult as the subject matter of the information may mean that the data subject is still able to infer the identity of the third party.

2. When deciding whether it is reasonable to disclose without consent, the following should be considered:

a) Any duty of confidentiality owed to the third party (i.e. consider the nature of the data and if the third party provided this information to the school on an understanding of confidentiality).

b) Any steps taken to obtain the third party's consent.

c) Whether the third party is capable of giving consent.

d) Any express refusal of consent by the third party and the reason for the refusal.

3. If the third party has not consented, this does not mean that personal data should be automatically withheld. Their reason for the refusal should be sought, as these reasons will determine whether it is reasonable in all the circumstances to withhold information that identifies them. For example, it may be reasonable to withhold data where the third party justifiably believes that disclosure may lead to physical retribution by the requestor. However, it may not be reasonable to withhold an individual's name if they have been acting in a work capacity and the documents show inability or incompetence in work which they are accountable for.

4. If the person handling the request decides that the data identifying the third party should not be provided, only that information which identifies the third party (either explicitly in the document or as the source of the information) may be withheld. This may require documents to be edited, either by blocking out third party identifiers or by retyping the information with third party details omitted.

2.4.2 Providing information in an intelligible form (s.7(1)(c) DPA)

1. Data subjects are entitled to be provided with a copy of their personal data in an intelligible form, with any codes, abbreviations or technical terms explained. When providing computerised information check that there are no codes that would require an explanation so that the individual can understand what they mean in relation to them.

2. This also means that if the requestor is a child or someone who lacks the mental capacity, then the information may need to be explained in simpler terms than when dealing with an adult.

2.5 Dispatch and Completion

2.5.1 Dispatch

1. Before sending the data, check:

a) Whether the consent of any relevant third party has been obtained.

b) If not, whether the data has been edited to conceal the third party's identity, or

c) Whether it is reasonable to disclose the data without consent.

d) If the third party is a school employee acting in their professional capacity, it should be noted that employee names are normally disclosable. However, employee names may be removed where it is considered appropriate in the circumstances to do so (e.g. where this may put that employee in danger).

2. Ensure explanations of all abbreviations and codes have been provided, where relevant.

3. Copy the edited manual and computer data and, if there is a considerable amount of data it is advisable to compile a schedule of all documents to be disclosed.

4. Make a note on the relevant file of any information/documents that have not been provided in response to the request, stating the reason for the non-disclosure (e.g. third party data or the particular exemption that applies). This information will be of assistance if your school receives a subsequent request or if we have to justify your decision to the Information Commissioner.

5. Send the requested copies of personal data together with a covering letter (Appendix 2 contains a template letter that can be adapted where necessary) to the applicant via recorded delivery, advising them:

a) That any query about the response should be referred back to the person who handled the request in the first instance.

b) Of any exemptions that have been relied if withholding information (unless the disclosure of the particular exemption would cause prejudice – e.g. to a criminal investigation).

c) That if they are dissatisfied with the way their subject access request has been dealt with, they can ask the Information Commissioner to undertake an assessment of how their request has been handled.

3 Exemptions to the right of access under the Data Protection Act 1998

1. There are limited exemptions to the right of subject access which allow information to be withheld from an applicant. However, they should be approached with caution, and applied on a case-by-case basis.

2. This section will only cover those exemptions that may apply to schools. In complex cases seek legal advice before withholding (or disclosing) information.

3. There is no exemption from disclosing embarrassing comments and in the majority of cases such comments will have to be released.

3.1 Disproportionate effort (section 8(2)(a) DPA)

1. This exemption has a limited effect as it only relates to the effort of providing a permanent copy of the information. A school will still be required to allow the individual access to view their personal data if a copy can not be provided. However, allowing a viewing can be problematic as there may be exempt information in the computerised/manual records.

2. The term “disproportionate effort” is not defined in the Act, so it is a question of fact in each case. The following may be taken into consideration:

a) The cost of providing the information.

b) The length of time it may take to provide the information.

c) How difficult it may be for information to be provided.

3. These issues must be balanced against the effect that withholding the information would have on the individual. The greater the adverse effect, the less likely the exemption could be applied.

3.2 Repeated requests (section 8(3) DPA)

1. There is no requirement to comply with a request from an individual which is identical or similar to a previous request from them, unless a “reasonable interval” has elapsed.

2. Factors to consider when deciding what amounts to a “reasonable interval” are:
a) The nature of the data.

b) The purposes for which the data are processed.

c) The frequency with which the data are altered.

3. Caution should be exercised here as the individual may have only requested specific personal data in their original request, and their subsequent request could be for other personal data held.

3.3 Crime (section 29)

1. Section 29 allows information which is processed for investigating a potential criminal offence to be withheld following a subject access request if, by disclosing the information, an investigation would be significantly prejudiced. This is likely to apply if a school is working closely with the Police or other prosecuting body in respect of a particular individual.

2. Decisions on the withholding of personal data should be made on a case-by-case basis. Whoever is involved in the investigation should be consulted when the request is received.

3. The Information Commissioner's view is that there must be "a substantial chance rather than a mere risk that in a particular case the purposes (i.e. the investigation or assessment/collection) would be noticeably damaged". Therefore, information held by the school should only be withheld where it can be shown beyond doubt that current or future investigation would be prejudiced by such a disclosure.

5. Where redactions are made they should only affect the prejudicial information. Other information which would not prejudice an investigation should therefore be disclosed as normal in response to a subject access request.

3.4 Health, education and social work records (section 30)

1. Schools hold education records and other types of records relating to pupils to undertake their functions. They may also hold occupational health records for staff. There are only very limited reasons for withholding these records where a subject access request has been made, as explained below.

3.4.1 Personal data relating to an individuals' physical or mental health

1. In some instances, the applicant may not have seen this personal data (or may have only seen part of the records). This type of personal data may be exempt where the disclosure would be likely to cause serious harm to the physical or mental health of the individual themselves or any other person.

2. Before deciding whether this exemption under section 30 of the DPA applies, a school is obliged to consult the health professional responsible for the clinical care of the individual. It is the health professional's decision as to whether the health data can be disclosed and there is no discretion to disclose without a response from the health professional.

3.4.2 Personal data contained within education records

1. If the release of personal data contained within an education record would be likely to cause serious harm to the physical or mental health of the individual, or any other person, then that personal data may be withheld. Information that would reveal that the data subject is, or may, be at risk of child abuse should be withheld.

2. The author of the education record should be consulted prior to deciding whether to rely on this exemption.

3.4.3 Personal data contained within social work records

1. This type of personal data would be exempt from disclosure where the release is likely to prejudice the carrying out of social work because serious harm to the physical or mental health of the data subject or any other person could result from the disclosure.

2. The author of the social work record or lead social worker should be consulted prior to deciding whether or not to rely on this exemption.

3.4.4 Personal data held within occupational health reports

1. An employee (or former employee) may request access to their occupational health report. In such circumstances personal data can be exempt if the disclosure of the personal data is likely to cause serious harm to the physical or mental health of the data subject, or some other person.

2. The health professional who wrote the report should be consulted prior to relying on this exemption.

3.5 References (schedule 7, paragraph 1)

1. This section provides an exemption to subject access where the data subject is requesting access to confidential references written by school employees.

2. This exemption does not apply to references that a school has received. If the data subject is requesting access to references that a school has received, then regard should be had to the third party data provision (see section 2.4.1).

3. References for the purposes of internal transfers or promotions are not covered by this exemption.

3.6 Management forecasts and planning (schedule 7, paragraph 5)

1. Personal data processed for the purposes of management forecasting or management planning are exempt from subject access to the extent that disclosure would be likely to prejudice the planning or forecasting activity.

2. For example, information about plans to promote, transfer or make a worker redundant may be withheld if access would be likely to prejudice the conduct of a school's business.

3.7 Negotiations (schedule 7, paragraph 7)

1. Personal data which contain a record of the intentions of a school in relation to any negotiations with the individual are exempt from subject access to the extent that disclosure of that personal data would be likely to prejudice that school's position in those negotiations.

2. For example, a statement outlining the maximum amount of money that the school would be willing to give a data subject as an out of court settlement could be withheld under this exemption, whilst the negotiations are on-going.

3. Information about negotiations which have ended are unlikely to be exempt unless it can be shown that other on-going negotiations would be prejudiced by such a disclosure.

3.8 Legally professionally privileged information (schedule 7, paragraph 10)

1. If personal data consists of information in respect of which a claim to legal professional privilege could be maintained, then that data may be exempt.

2. Legal professional privilege applies to correspondence (e.g. letters, emails and memos) between school employees and qualified legal advisors for the purposes of obtaining legal advice.

3. For example this exemption could apply where an individual involved in litigation with a school is requesting access to the personal data contained within correspondence that the school has sent/received from a legal advisor.

4. Communications with lawyers (inc the Council's lawyers) are likely to be subject to legal professional privilege and must not be disclosed. If such documents are found whilst dealing with a subject access request, seek advice from the legal adviser concerned (or the Council's Data Protection Advisor).

3.9 What should you do if an exemption applies to the personal data?

1. If personal data is to be withheld under any of the exemptions then the reasons for the non-disclosure (including the exemption relied upon) should be documented on file so that the school can justify its actions to the Information Commissioner or the courts. Such reasons should normally be provided to the applicant, as well as an explanation of the way the application of the exemption can be challenged (See standard letter in Appendix 2).

2. The Crime exemption does not have to be cited in your response to the applicant, if notifying the applicant of the reliance placed on this exemption would cause prejudice to the criminal investigation.

3. Where an exemption applies only in part, then the information which is not exempt should be released to the data subject within the statutory time frame.

4 The Eight Data Protection Principles

1. The Eight Data Protection Principles are sometimes referred to as the 'principles of good information handling'; they represent the standards that schools (and other organisations holding personal data) are expected to comply with when using, obtaining and disclosing personal data. The principles are legally enforceable by the Information Commissioner or the courts.

4.1 Principle One: personal data shall be processed (i.e. used) fairly and lawfully and a condition for processing the personal data must be satisfied before the data can be used for that purpose.

1. For personal data to be processed fairly the individual should normally be given the following information:
a) The name of the data controller (i.e. the name of the school).
b) The purposes for which the school intends to use their personal data (if this is not obvious).
c) Whether the school intends to share/verify their personal data with other organisations (including naming who they are).

2. The information in (a)–(c) should normally be given to the individual at the point at which their personal information is collected (e.g. in application forms). However, where we have received information about an individual from a third party, the information specified above should be provided as soon as it is practical to do so.

3. For schools to lawfully process personal data they must only use the information it holds for activities connected with their statutory functions (e.g. under the various Education Acts). Schools must also ensure that the personal data they hold is only used for those purposes which are detailed in their notification with the Information Commissioner's Office (see http://www.ico.gov.uk/tools_and_resources/register_of_data_controllers.aspx for more information).

4. The final element of Principle One requires that the school satisfies one of the conditions contained within the Act before using the personal data. One of those conditions is to gain consent from the data subject, but this may not be appropriate or obtainable in all circumstances. The consent of the individual is not always needed for the school to use personal data while carrying out its work.
5. The Act provides a number of other conditions of equal value that schools may be able to rely upon. For example, where the use of the personal data in a particular way is required in order to ensure that the school fulfils its statutory obligations, or alternatively where there is a substantial public interest in the disclosure of personal data to a third party.

6. Sensitive personal data (see below) must also satisfy a further condition from a second list. In the same way as above it is likely that sensitive personal

data processed for fulfilment of the school statutory functions would be covered by the condition that the processing is necessary “for the exercise of any functions conferred on any person by or under any enactment”.

7. Sensitive personal data is personal data about any of the following;
a) the racial or ethnic origin of the data subject,

b) his political opinions,

c) his religious beliefs or other beliefs of a similar nature,

d) whether he is a member of a trade union

e) his physical or mental health or condition,

f) his sexual life,

g) the commission or alleged commission by him of any offence, or

h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

4.2 Principle Two: personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

1. This means that schools are not normally able to use personal data for a purpose that is wholly unrelated to the purpose for which the data was originally collected.

4.3 Principle Three: personal data shall be adequate, relevant and not excessive.

1. The amount of data stored on individuals must be justifiable. Personal data should not be collected merely on the basis that there is a slim chance that it will be of use.

2. Every care should be taken to ensure that the information schools collect from individuals is relevant for the purpose(s) it is required.

4.4 Principle Four: personal data shall be accurate and, where necessary, kept up to date.

1. Inaccurate data may compromise the integrity of operations, causing schools to be subjected to unnecessary litigation, and cause irritation, resentment and suspicion amongst data subjects. Methods must be established for verifying data and if information is unclear it should be checked.

2. Every care should be taken to ensure that the information recorded on individuals is entered accurately.

4.5 Principle Five: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

1. This principle suggests that good 'housekeeping' practices need to be adopted and rules concerning minimum time periods relating to the retention of data must be complied with. Personal data should not be retained indefinitely simply because it might be of some use in the future. However, information may be used by more than one department and should not be deleted unless all business needs have been met.

2. Data should be retained for as long as it is necessary for all our business needs and then destroyed or archived in accordance with school's retention policy.

4.6 Principle Six: personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

1. Individuals have a number of rights given to them under the Act and it is a breach of the Act if a school fails to comply where those rights that have been exercised.

2. Such rights include: the right to have a copy of their personal data, rights in relation to automated processing, and rights in relation to the prevention of processing in certain circumstances.

3. Individuals can contact the Information Commissioner's Office to obtain leaflets explaining all of their rights (see http://www.ico.gov.uk/for_the_public.aspx for more information).

4.7 Principle Seven: appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1. In considering what would be reasonable security measures the Act provides a number of issues that can be taken into account; the cost of security, the risks involved, the sensitivity and value of the data and the harm that could result if the information was misused, lost or accidentally destroyed. When considering what level of security is required it is worthwhile considering the following balance:

cost and available technology
type of data and possible harm if lost or misused

2. In terms of schools, this means that you must ensure that your systems that hold personal data are secure and that employees who handle the personal data are properly vetted and trained. You must also ensure that the school uses personal information in a way which is secure. Transferring information is one of the least secure parts of data handling.

3. Where a school uses a third party to manage personal data on its behalf (data processors), it must ensure that the third party has appropriate security measures in place to protect the personal data. The security standards that data processors agree to must be enforceable through contractual terms (seek advice from the Council's Data Protection Advisor if necessary).

4. Schools must ensure that any personal data held, either at the school premises, or on a laptop if working from home, is secure and free from unauthorised disclosure. This includes making sure that family or friends do not use or have access to school laptops.

5. Laptops/files must not be left unattended if removed from school premises and must be kept secure especially while travelling.

4.8 Principle Eight: personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1. If you are, or are considering, sending personal data outside of the European Economic Area (the European Union countries plus a few others) seek advice from the Council's Data Protection Advisor before doing so.

Appendix 1 – Standard letter to an applicant seeking a fee and/or additional information to locate their personal data/prove their identity.

Our reference:

[Name]
[No. Street]
[Town]
[City]
[Postcode]

Date:

Dear Mr/Mrs/Miss/Ms

Access to personal data under the Data Protection Act 1998

Thank you for your [letter/email] of [dd/mm/yy] requesting information that the school holds about you in its computer systems and manual files.
(*Delete paragraphs if not appropriate)

***Seeking payment**
[Under section 7(2)(b) of the Data Protection Act 1998 a fee of £10 is payable before I can deal with your request for your personal information. Please make your cheque or Postal Order payable to the "*Enter the name of your school*", and send it to me at the above address, clearly marking your letter "Data Protection Act 1998 – Subject Access Request ".]

(*The paragraph below should be used if you are in any doubt about the identity of the person claiming to be the data subject making the subject access request, and you are concerned about the damage or distress that would result to the real data subject if data was accidentally disclosed to the wrong person. Otherwise it is safe to rely on the usual signature of the individual as proof of identity and information sent to the known address we have on file).*

***Seeking further proof of identity**
[As some of the information we have about you may be sensitive, for security reasons, I would be grateful if you would provide one further form of identification. This could be:
A witness to your signature by someone who is over 18 and is not a relative, (preferably by your doctor/solicitor on their headed business paper);
A copy of your birth certificate;
A copy of your passport.]

***Seeking reasonable additional information to locate data**
[Your request for all personal data that we may hold on you is very vague, and I would be grateful if you would let me know more specifically what

information you are seeking, and/or provide any other information that would enable me to locate it, such as:
Details of your involvement with school;
Dates of your involvement with the school (i.e. from xxxx to xxxx);
Any reference numbers that the school has included in correspondence to you (if known).

You may already have seen some of the information that the school holds on you. If you do not wish to receive copies of correspondence that have previously been sent to you, please let me know otherwise they will be provided again. If there is any specific information that you require, please indicate this and provide sufficient details to enable me to locate it, such as the subject matter of any document, date, and the relevant person dealing with it (if known).

Once I have received your reply, your request will be dealt with as quickly as possible and, in any event, within the 40-day limit set by the Act. The 40 days will start from the date I receive the fee and/or the additional information* that I have asked you for in this letter.

*** delete as appropriate**

Yours sincerely

Appendix 2 – Standard response letter to a subject access request.

Our reference:

[Name]
[No. Street]
[Town]
[Postcode]

Date:

Dear Mr/Mrs/Miss/Ms

Access to personal data under the Data Protection Act 1998

Thank you for your letter of [dd/mm/yy] requesting information that the school holds about you. I confirm that we have received the fee of £10.

I confirm that the school does hold information about you. Our records show that [explain briefly the nature of the records held on the applicant and their relationship with the school].

I enclose copies of your personal data held on our computer system and in our manual files.

Where abbreviations have been used in a document, these are explained in full. Any text that may be missing from the computer screen printouts have been typed in full so that you can see the complete details recorded.

Any information that has been received from third parties about you has also been provided, subject to any duty of confidentiality we owe to the third party concerned. This may mean that some documents could have had information erased if they contain personal details about the third party and their consent to the disclosure has been withheld.

[Identify if any personal data has been withheld on the basis of one the DPA exemptions].

If you have any questions about the data I have provided to you, please do not hesitate to contact me.

Should you be dissatisfied with the way in which your subject access request has been handled you may ask the Information Commissioner (the independent regulator of the Data Protection Act) to carry out an assessment of how your request has been handled. The Information Commissioner can be contacted by writing to:

Information Commissioner's Office
Wycliffe House
Water Lane

Wilmslow
Cheshire
SK9 5AF

Information Commissioner enquiry line: 01625 545745

Yours sincerely

Appendix 3 – Fees chargeable for manual education records held by the school.

Number of pages of information comprising the copy	Maximum fee
Fewer than 20	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-69	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500 or more	£50

Appendix 4 – useful links to other guidance

Access to Pupils Information held by schools in England - http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/technical_guidance_note_access_to_pupils_information_held_by_schools_in_england.pdf

Subject access requests and third party information considerations - http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/sar_and_third_party_information_100807.pdf

Subject access and employment references – http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/subject_access_and_employment_references.pdf

Individuals' rights of access to examination records – http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_good_practice_note_access_to_exam_results.pdf

Publication of exam results by schools - http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/disclosure_of_examination_results_to_the_media_final_web_version.pdf

Taking photographs in schools good practice note - http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/taking_photographs_in_schools.pdf

Lambeth Council's subject access policy – http://www.lambeth.gov.uk/Services/CouncilDemocracy/DataProtectionFOI/DataProtection_EXTRA.htm

Lambeth Council's Data Protection policy – http://www.lambeth.gov.uk/NR/exeres/68409BE6-5EA1-4240-A8C0-542A4C9F35F4.htm

Example Data Protection policy for schools - http://services.bgfl.org/services/datapro2/files/sample.pdf