LANGDON
PRIMARY SCHOOL

Data Protection Policy (incorporating Access to Information Requests)

Created Spring 2016

Agreed by the Curriculum Team of the Governing Body 3.2.16

Due for review Spring 2018

Introduction

The Data Protection Act came into force in 1998. It sets out what can and cannot be done with personal data that is, information about living individuals.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. All staff must be aware of and ensure that they comply with the requirements of the Act.

Commitment to the Protection of Personal Information

Staff and Governors at Langdon Primary School need to collect and use certain types of information about people with whom they deal in order to operate effectively. These include pupils, parents and carers, staff, governors, outside agencies concerned with education, child health or welfare, suppliers and others with whom the school communicates. In addition, we are required by law to collect and use certain types of information to comply with the requirements of government departments.

Personal information must be dealt with properly and securely regardless of which method is used for collection, recording or use – whether this is through a paper or computerized system. Langdon Primary School is committed to working within the guidelines for Data Protection issued by the Local Authority and by the Information Commissioner.

Langdon Primary School regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions and to maintaining confidence between those with whom we deal and ourselves.

Data Protection Principles

The Data Protection Act is based on eight principles for ‘good information handling’ which must be adhered to. At Langdon Primary School we have adopted these principles for our own use and ensure that:

1. Data will be processed fairly and lawfully

2. Personal data shall be obtained only for one or more specific and lawful purposes

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed

4. Personal data shall be accurate and where necessary kept up to date.

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.

7. 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.

8. Personal data shall not be transferred to a country outside the EEA, 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.

Notification

To comply with the principles of the Data Protection Act schools must register their reasons for processing personal data with the Information Commissioners Office; this process is called Notification. Failure to notify is a criminal offence. Notification is updated annually and the school submits necessary returns in a prompt and timely manner.

Responsibilities

The Governing Body is ultimately responsible for ensuring the school implements the principles of the Data Protection Act. The governors have delegated the day to day management of these principles to the school's designated Data Controller, the Head Teacher - Lynn Paylor Sutton.

The Head Teacher is responsible for ensuring that all members of the school community, who collect information about individuals, comply with the Data Protection Principles as set out above.

Staff, governors, parents and others connected with the school are responsible for checking that any information they provide to the school in connection with their employment, role within the school or their child's education and well-being is up-to-date and accurate. Individuals should inform the school promptly of any changes to the information they have provided. The school cannot be held responsible for any errors if they have not been informed of such changes.

Data Security

All personal data, whether held in a paper or computerized system, must be kept securely in order to prevent accidental loss, damage or destruction. The extent of the security measures required will depend upon the sensitivity of the data.

Paper records should be kept in a lockable drawer, filing cabinet, cupboard or safe. Keys should be kept in a safe place. Paper records should never be left unattended where they might be visible to individuals who are unauthorized to view them. If staff take paper records home they should ensure that they are not left unattended and that they are never left in cars overnight.

If the data is held electronically then access should be password protected. Staff should ensure that PC screens cannot be viewed by individuals who are not authorized to view the data. PCs should be locked or switched off when not in use.

Staff who use laptop computers or data memory devices in their work at school should ensure that they are not used by unauthorized individuals who could access personal data stored on them. Staff should ensure that data devices and laptops are not left unattended for any length of time and should be vigilant about where they are stored both in school and if using them at home, in particular staff must ensure that they are never left in cars overnight. Home PCs should not be used for the storage of any personal data.

Personal data sent from the school to external organizations should be clearly addressed to the recipient and labeled 'confidential'. Personal data should only be sent via e-mail as an attachment and flagged 'confidential'. Personal data should not be faxed unless staff are sure that receiving fax machine is a 'safe haven' machine which is locked when unattended.

When records containing personal information have reached the end of their necessary life, they should be disposed of by shredding, incineration or by using confidential waste bins provided by the Local Authority. Staff should be mindful of the guidance from the Local Authority on timescales for retaining information in school before disposing of data. These timescales are available in the school office, on Kent Trust Web or directly from the Local Authority.

As a guiding principle, staff should ensure that at all times personal information relating to individuals is treated as they would wish their own data to be treated.

Rights of Access to Information

All staff, governors, pupils and parents and others connected with the school are entitled to:

- Know what information the school holds and processes about them or their child and why;
- Know how to gain access to it;
- Know how to keep it up to date;
- Know what the school is doing to comply with the Data Protection Act.

Information requested falls into two categories – subject access requests and personal data access requests.

Any individual, including pupils at the school, has a right by law to access certain personal data which is kept in school about them. Any person who wishes to exercise their right to access personal data which is classed as being part of the education record should discuss it with the Head Teacher, as the designated Data Controller, and submit a formal request in writing following that discussion. The school aims to comply with requests for access to personal information within the education record as quickly as possible, but

will ensure that a hard copy is provided within fifteen school days as required by the Data Protection Act.

Any person who wishes to make a secure access request should also discuss it with the Head Teacher and submit a formal request in writing following that discussion. The response time for subject access requests, once officially received, is forty days (not working or school days, but calendar days, irrespective of school holiday periods). However, the forty days does not begin until after the fee for providing information under a subject access request and any further information required, eg. identity verification documents, is received.

The school will charge a fee on each occasion that access is requested according to current Local Authority recommendations for charges for such a service (the school will charge the maximum recommended fee for each category).

The Data Protection Act applies to people of all ages. In the case of pupils, if the child is able to understand what is being asked of them they should be given the opportunity to give their own consent with regard to Data Protection issues. This is known in law as the 'Gillick Principle'. Former pupils of the school may be asked for information to verify their identity or for information which would help locate the data held about them eg. dates between which they attended the school, before being given access to personal information held by the school.

Excepted personal data which will not be disclosed to individuals requesting to exercise their right to access personal data, is information relating to safeguarding, specifically child protection, as detailed in local authority guidance and in the interests of the safety and well being of the child.

Subject Consent

In many cases the school can only process personal data with the consent of the individual. Sometimes it is necessary to process information of a sensitive nature, eg. information about health, race, criminal convictions. This may be to ensure that the school is a safe place for everyone, to ensure that the school's legal obligations are met or to operate other school policies such as the Equal Opportunities Policy, First Aid and Medical Needs Policy or Pay Policy. Individuals will be asked to give their express consent for the school to process this data. For staff, in some cases, an offer of employment can be withdrawn if an individual refuses to consent to processing of information without good reason.

Disclosure of Personal Data

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

All disclosures must be in accordance with the school's Notification and with the consent of the individual to whom the data refers. If consent is required

but has not been obtained, disclosure can only take place if the personal data has been anonymized.

Where disclosure is permitted staff should always take appropriate action to ensure the identity of those they disclose to. Disclosure over the telephone is strongly discouraged and callers should be invited to put the request in writing. If a request is urgent then staff should take note of the caller's name and telephone number and verify their details before responding.

If a member of staff is in any doubt about disclosure they must seek advice from the Head Teacher.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.