

# **Judith Kerr Primary School**

## **Data Protection Policy**

**May 2016**

**Review by: April 2018**

## Introduction

1. In order to operate efficiently Judith Kerr Primary School has to collect and use information about people. This may include current, past and prospective pupils, parents, members of the public, staff and suppliers.
2. The School is committed to ensuring personal data is properly managed and the Data Protection Act 1998 (DPA) is complied with. The School will make every effort to meet its obligations under the legislation.

## Scope

3. This policy applies to all staff, governors, contractors, agents and representatives working for or on behalf of the School and is available to all others in the school community via the website and on request. This policy can be made available in large print or other accessible format if required.
4. This policy applies to all Personal Data processed by the School and held electronically or manually.
5. Images captured by individuals for personal or recreational use with a mobile phone, digital camera or camcorder are exempt from the DPA (i.e. parents are allowed to take photos of pupils in a school play).

## Responsibilities

6. The school is the data controller for the purposes of the act and therefore the governors have overall responsibility for compliance with the DPA.
7. The governors have delegated responsibility to the headteacher for ensuring compliance with the DPA and this policy within the day-to-day activities of the School.
8. The headteacher has appointed the School Administrator to act as the school's Data Protection Officer (DPO). The DPO is responsible for:
  - notifying the Information Commissioner's Office (ICO) and renewing the school's registration annually;
  - keeping the ICO up to date with changes in how the school processes data;
  - obtaining consent for disclosure of Personal Data, including routine consent from parents and pupils for using photographs for general school purposes;
  - ensuring data protection statements are included on forms that are used to collect Personal Data;
  - acting as a central point of advice for staff on data protection matters;
  - co-ordinating requests for personal data;
  - arranging appropriate data protection training for all staff;
  - keeping up to date with the latest data protection legislation and guidance;
  - ensuring adequate systems are in place for compliance with this policy.

## Definitions

9. **Personal Data:** information which relates to an identifiable living individual that is processed as data. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.
10. **Processing data:** collecting, using, disclosing, retaining, or disposing of information.
11. **Sensitive Personal Data:** information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

## **The requirements**

12. The DPA stipulates that anyone processing Personal Data must comply with eight principles of good practice. The principles require that Personal Data:
- shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
  - 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;
  - shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
  - shall be accurate and where necessary, kept up to date;
  - shall not be kept for longer than is necessary for that purpose or those purposes;
  - shall be processed in accordance with the rights of data subjects under the Act;
  - shall be kept secure i.e. protected by an appropriate degree of security;
  - shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

## **Notification**

13. As required under the DPA, the School will ensure that the ICO is notified that the School is processing Personal Data and in what ways, and the School shall ensure that this notification is kept up to date and renewed annually.

## **Data Gathering**

14. Whenever the school collects new information about individuals we will ensure individuals are made aware:
- that the information is being collected;
  - of the purpose that the information is being collected for;
  - of any other purposes that it may be used for;
  - who the information will or may be shared with; and
  - how to contact the data controller.
15. The School will only obtain relevant and necessary Personal Data for lawful purposes and will only process the data in ways which are compatible with the purpose for which it was gathered.
16. Data Protection statements will be included in the school prospectus and on forms that are used to collect personal data.

## **Data storage**

17. Personal Data will be stored in a secure and safe manner. The following measures are taken to help ensure this:
- electronic data will be protected through secure password, encryption software and firewall systems operated by the school;
  - computer workstations in administrative areas will be positioned so that they are not visible to casual observers;
  - Manual Personal Data will be stored securely where it is not accessible to anyone that does not have a legitimate reason to view or process the data;
  - particular attention will be paid to the need for security of Sensitive personal Data, for example health and medical records will be kept in a locked cupboard;
  - Personal Data will not be left out visible on desks;

- the physical security of school buildings and storage systems will be regularly reviewed;
- staff will be trained on this policy and related data protection procedures.

### **Data checking**

18. Systems will be put in place to ensure the Personal Data that the school holds is up to date and accurate. For example the School will ensure that parents are asked at least once a year to confirm their contact details.
19. Any inaccuracies discovered or reported will be rectified as soon as possible.

### **Disclosing Data**

20. Personal Data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
21. When requests to disclose Personal Data are received by telephone, the school will ensure that the caller is entitled to receive the data and that they are who they say they are. In some circumstances the school may call the caller back to check the identity of the caller.
22. Personal Data will not be included on the website, in newsletters or other media without consent of the individual (or his/her parents where appropriate). Routine consent may be requested from parents to avoid the need for frequent, similar requests for consent being made by the school.
23. Personal Data will only be disclosed to the Police if they are able to supply a WA170 form which notifies of a specific, legitimate need to have access to specific Personal Data.

### **Data Subject Access Requests**

24. Any person whose Personal Data is held by the School is entitled, under the DPA, to ask to access this information. The request must be in writing. The right is to view or be given a copy of the Personal Data, rather than to the whole document which contains the Personal Data.
25. There are some exceptions to the rights of access to information in certain records held by the school (for example in relation to examination scripts, legal advice).
26. When a request is received by a member of staff, this should be passed to the school's Data Protection Officer without delay. The request must be dealt with promptly; a response must be provided as soon as possible and no later than within 40 calendar days from the date the request was received.
27. The School may make a charge of £10 for responding to a request for Personal Data under the DPA and will need to confirm the requester's identity.
28. Parents can make data subject access requests on their child's behalf if their children are deemed too young to look after their own affairs. If a request is made by a parent for Personal Data relating to their child and the child is aged 12 years or older, written consent will need to be sought from the child before the data is disclosed to the parent.
29. A record will be kept of all data subject access requests made that require formal consideration.

### **Destroying data**

30. Out-of-date information will be discarded if no longer relevant. Personal Data will only be kept as long as reasonably needed, for legal or business purposes.

### **Breach of the policy**

31. Non-compliance of this policy and data protection legislation by a member of staff is considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

### **Monitoring, evaluation and review**

32. The Headteacher will report back to the Governing Body on this policy and its implementation and effectiveness every two years, who will then review the policy, making amendments where necessary.