



Leighfield

**Leighfield Academy**

## Data Protection Policy

Adopted by the Governing Body 19<sup>th</sup> November 2013

# Leighfield Primary School

## Data Protection Policy

### **Policy Statement:**

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

### School Aims

Leighfield School aims for children to

- ◆ Reach their full potential
- ◆ Develop a positive self-image
- ◆ Be responsible and make informed choices

We

- ◆ Provide a supportive and caring environment
- ◆ Promote high achievement
- ◆ Encourage independent learning

### **Introduction**

Leighfield Academy needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act).

In summary these state that personal data shall:

- ◆ Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- ◆ Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- ◆ Be adequate, relevant and not excessive for that purpose.
- ◆ Be accurate and kept up to date.
- ◆ Not be kept for longer than is necessary for that purpose.
- ◆ Be processed in accordance with the data subject's rights.
- ◆ Be kept safe from unauthorised access, accidental loss or destruction.

All staff or others who process or use personal information must ensure that they follow these principles at all times.

Leighfield Academy is registered with the Information Commissioners Office, as required by The Data Protection Act 1998. We refer to their written code of practice.

### **Status of this Policy**

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

### **The Data Controller and the Designated Data Controllers**

The School as a body corporate is the Data Controller under the 1998 Data Protection Act, and the Governors are therefore ultimately responsible for implementation.

However, the Designated Data Controllers will deal with day to day matters.

The Schools have three Designated Data Controllers: the Headteacher, School Business Manager, and the School Administrator.

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

### **Responsibilities of Staff**

All staff are responsible for:

- ◆ Checking that any information that they provide to the school in connection with their employment is accurate and up to date.
- ◆ Informing the school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.
- ◆ If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with Data Protection Guidelines.

Staff have been consulted on this policy and a copy is stored on the school intranet.

### **CCTV**

- ◆ Recording images of identifiable individuals is processing personal information.
- ◆ Cameras are only sited where they are for the intended purpose and do not intrude unnecessarily on anyone's privacy.
- ◆ Footage is stored for.....
- ◆ The premises officer has access to this footage on a day to day basis. He would inform a Designated Data Controller if he felt the data needed to be shared more widely, eg with the police.

### **Permission**

Permission is sought from parents to publish a pupil's name or photograph in the newspaper or on the website.

### **Data Security**

All staff are responsible for ensuring that:

- ◆ Any personal data that they hold is kept securely.

- ◆ Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- ◆ Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

## **Storage**

Personal information should:

- ◆ Be kept in a locked filing cabinet, drawer, or safe; or
- ◆ If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- ◆ If a copy is kept on a removable storage media, that media must be encrypted and kept in a locked filing cabinet, drawer, or safe.
- ◆ No sensitive data must ever be left unattended in a car.

## **Data Checking**

The CTC will issue regular reminders to staff and parents/carers to ensure that personal data held is up-to-date and accurate.

Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

## **Data Disclosures**

- ◆ 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.
- ◆ When requests to disclose personal data are received by telephone it is the responsibility of the member of staff taking the call to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- ◆ If a personal request is made for personal data to be disclosed it is again the responsibility of the member of staff to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- ◆ Requests from parents/carers or students for printed lists of the names of students in particular groups, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the students are present in class will resolve the problem.)
- ◆ Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- Routine consent issues will be incorporated into the CTC's student data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the CTC.
- Personal data will only be disclosed to Police Officers if they are able to supply a relevant document which notifies of a specific, legitimate need to have access to specific personal data. The document used by West Midlands Police is called a WA170 and must be signed by someone the rank of an inspector or above. Other forces' will use differently named forms.

- A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

### **Rights to Access Information**

All staff, parents and other users 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 its obligations under the 1998 Act.

The school will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the school holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should put their request in writing to the school.

The School will make a charge of £5 on each occasion that access is requested if the request is for paper copies of a file containing the required information, although the School has discretion to waive this.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 working days, as required by the 1998 Act.

### **Subject Consent**

In many cases, the school can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained.

Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions, in accordance with our policy of employment of Ex-Offenders. The school has a duty of care to all staff and students and must therefore make sure those employees and those who use School facilities do not pose a threat or danger to other users. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes.

The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency.

### **Publication of School Information**

Certain items of information relating to school staff will be made available via searchable directories on the public web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school.

**Retention of Data**

The School has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

**Disposal of Data**

- ◆ Paper records will be shredded
- ◆ Electronic data will be deleted

**Conclusion**

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Related Policies: Recruitment of Ex-Offenders, Personal Information Policy