

# CALSHOT PRIMARY SCHOOL

## Data Protection Policy



'At Calshot we aim to provide the highest quality of learning and care for ALL children in a safe and enjoyable environment, nurturing personal values, in partnership with parents, carers and the wider community. We expect everyone in our school to strive to achieve their full potential'

## Calshot Primary School - Data Protection Policy

The school will comply with:

- The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
- Birmingham Education Service advice and guidance supplied in *Data Protection Guidance for Schools* booklet.
- Information and guidance displayed on the Information Commissioner's website ([www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)).

This policy should be used in conjunction with the school's *Internet and E-Mail User Policy*.

### **Data Gathering**

- All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
- Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

### **Data Storage**

- Personal data will be stored in a secure and safe manner.
- Electronic data will be protected by a standard password and firewall systems operated by the school.
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
- Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.

### **Data Checking**

- The school will issue regular reminders to staff and parents 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 will be 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 organizations 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 school 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 school 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.
- If there is a requests from parents or children for printed lists of the names of children in particular classes, only the first names will be given
- 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 school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.
- Personal data will only be disclosed to Police Officers if they are able to supply a WA170 form which gives notice of a specific, legitimate need to have access to specific personal data. This form is the agreed procedure between Birmingham City Council and West Midlands Police.
- A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

## Data Destruction

- Data will be destroyed in line with guidelines issued by the 'Records Management Society of Great Britain' which legislates how long data needs to be retained for.

## Subject Access Requests

- If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 day deadline.
- Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time, but in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40 day time limit.

### **Roles within School**

- Senior Information Risk Officer - W.Simner (Head Teacher)
- Assessment Information Officer - M.Wingrove (Deputy Head Teacher)
- Data Manager / MIS Manager - M.Wingrove (Deputy Head Teacher)
- Data Protection / Freedom of Information Nominated Person - W.Simner (Head Teacher)

Policy revised by W.Simner (Head Teacher) in June 2016

Policy ratified by the Governing Body on 4<sup>th</sup> July 2016

