

DATA PROTECTION POLICY

The Data Protection Act 1998 which replaced the 1984 Act, received Royal assent on 16th July 1998 and came fully into force in 1999.

As with the 1984 Act, the Act gives legal rights to individuals (data subjects) in respect of personal data held about them. The Act gives effect in UK law to EC Directive 95/46/EC (the Directive).

Purpose of the Data Protection Act

The Data Protection Act 1998 is designed to cover the collecting, storing, processing and distribution of personal data. It gives rights to individuals about whom information is recorded.

This applies to all individuals whether they are an employee, elected member or a member of the public. Each individual has the right to access personal data, prevent processing likely to cause damage or distress and prevent processing for the purposes of direct marketing.

They also have rights in relation to automated decision taking, to take action for compensation if they suffer damage by any contravention of the Act by the data controller, to rectify, block, erase or destroy inaccurate data and to make a request to the Data Protection Commissioner for an assessment to be made of the data controller if they feel that the Act has been contravened.

The Act places obligations on those who record and use personal data (data controllers). They must be open about the use of such personal data through notification to the Information Commissioner and they must follow sound and proper practices by applying the Data Protection Principles.

General Statement

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The School leadership team and Governors of this School seek to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the school's Data Protection Policy is available from school office. General information about the Data Protection Act can be obtained from the Data Protection Commissioner (Information Line 01625 545 745, website www.dataprotection.gov.uk).

Fair Obtaining and Processing

St Joseph's Catholic Primary School, Poole undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the

purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

“Processing” means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

“Data subject” means an individual who is the subject of personal data or the person to whom the information relates.

“Personal data” means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

“Parent” has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Registered Purposes

The Data Protection Registration entries for the School are available for inspection, by appointment, at the school office. Explanation of any codes and categories entered is available from Hilary Barker who is the person nominated to deal with Data protection issues in the School. Registered purposes covering the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity

The school undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for

missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of Hilary Barker (*Data Protection nominated officer*) to ensure that obsolete data are properly erased. A schedule for disposal of data is located in school office.

Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

- ◆ Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form, available from the School Office. Completed forms should be submitted to Hilary Barker (*the nominated officer*). Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school dates in accordance with the current Education (Pupil Information) Regulations.

Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- ◆ Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations. E.g. EWO
- ◆ Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare. e.g. Social Care
- ◆ Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

- ◆ Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- ◆ Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A “**legal disclosure**” is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An “**illegal disclosure**” is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

Data and Computer Security

St Joseph's Catholic Primary school, Poole School undertakes to ensure security of personal data by the following general methods:

Physical Security

- Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the office. Computers are locked with personal passwords which are not readily available and stored securely in a locked safe.
- Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.
- Printed data needs to be kept secure. Admin and Safeguarding staff need to lock paper copies when not protected by staff presence. Teaching staff need to ensure that files containing data are kept secure.
- **The office areas must have restricted access to protect data.** The doors to the office need to be shut and computers are locked at all times when left unattended to protect data. Computer screens are situated to avoid easy viewing.
- Verbal communication regarding pupil data is handled with care to ensure that visitors to the school are not able to hear the information.
- Admin and teaching staff are cautious to ensure that parents/visitors/contractors etc waiting in the entrance area or at hatch

are NOT able to **hear** or **see** information that is subject to data protection.

- Teachers and teaching assistants are mindful to avoid visitors and parent helpers in school having access to data stored in files in classrooms or other areas of the school.
- During parent/ carer Consultations: staff ensures that personal data is not visible to other parents.
- **Transfer of data and communication that identifies pupils MUST be carried out using the secure Poole Gateway.**

Logical Security

- Security software is installed on all computers containing personal data.
- Only authorised users are allowed access to the computer files and password changes are regularly undertaken.
- Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

- In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement and a user policy in line with e safety and data policies. All staff are trained annually in their Data Protection obligations and their knowledge updated as necessary.
- Computer printouts containing data as well as source documents are **shredded** before disposal.
- Staff are provided with encrypted memory sticks to save data that they may create at home.

Overall security policy for data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to Hilary Barker (the person responsible). A log of concerns will be completed to address any potential breaches.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from: Hilary Barker DATA PROTECTION OFFICER
Information regarding data protection are located on the school website.

Date of issue/revision: 10.09.12

Reviewed and agreed by governing body:

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname.....

Enquirer's ForeNames.....

Enquirer's Address

.....
.....
.....
.....

Enquirer's Postcode

Telephone Number

Are you the person who is the subject of the records you are enquiring about

YES / NO

(I.e. the "Data Subject")?

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the

YES / NO records you are enquiring about?

If YES,

Name of child or children about whose personal data records you are enquiring

.....
.....
.....
.....

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information.

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

.....

Name of "Data Subject" (or Subject's Parent)

(PRINTED).....

Dated

.....