

Engayne Primary School

Data Protection Policy

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 Headteacher and Governors of the School intend 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. Engayne Primary School has an Information Commissioner's office (ICO) certificate of registration.

Enquiries

Information about the school's Data Protection Policy is available from the Headteacher, or School Business Manager. General information about the Data protection Act can be obtained from the Data Protection Commissioner (www.dataprotection.gov.uk or their telephone contact).

Fair Obtaining and Processing

Engayne Primary School undertakes to obtain and process data fairly and lawfully by informing all data subject 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 related 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 the School Finance officer 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 disclosure 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 the 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. (Details should be added on how and when records are checked for irrelevant data and who has the say on what must be deleted).

Length of time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the School business manager to ensure that obsolete data are properly erased.

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 pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.
- 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 the school business manager. (See appendix 1)

A written request from a parent regarding their own child's record, access to the record will be provided within 15 school days 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 in 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.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their children's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- 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 working on behalf of the LEA are IT liaison/data processing officers and are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosure 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 not right to it, or one which falls outside the School's registered purposes.

Data and computer security

Engayne Primary School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed).

Physical security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. All data is locked away securely, when not in use. Visitors to the school are required to sign in and out, wear identification badges whilst on the school premises and are, where appropriate, accompanied.

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 regularly.

Procedural security

In order to be given authorised access to the computer, staff will have undergone checks. All staff are trained in their Data Protection obligations (staff guide appendix 2) and their knowledge updated as necessary. Computer printouts as well as source documents are sent for confidential disposal.

Overall security policy for data is determined by the Headteacher/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 the school business manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter and serious breaches could lead to dismissal.

Date of Issue: May 2016

Access to personal data request

Date Protection Act 1998 Section 7.

Enquirer's SurnameFirst Names

Enquirer's Address

.....

Telephone Numbers

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 the child who is the "Data Subject" of the records you are enquiring about? YES/NO

If YES

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

.....

Description of Concern / Area of Concern

.....

.....

Description of Information of Topic(s) requested (In your own words)

.....

.....

Additional Information

.....

Please despatch reply to: (If different from enquirer's details as stated on this form)

.....

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's" parent or guardian.....

Names of "Data Subject's" parent or guardian (PRINTED)

Date:

Data Protection at Engayne Primary School

Engayne ensure staff understand the basics of information governance; recognise where the law and good practice need to be considered and know where to turn for further advice.

Personal Data – Engayne identify the need to handle personal information in line within recognised data protection principles.

Fair Processing – Engayne let individuals know what we do with the personal information we record about them. We do not to disclose personal information without consent or within the Freedom of Information guidelines.

Sharing – Engayne restrict sharing information to only necessary parties. We make sure those we share with also work within recognised data protection principles.

Security – keep confidential information secure when storing it, using it, sharing it and disposing of it.

Anyone who processes personal information must comply with eight principles of the Data Protection Act which make sure that personal information is:

- Fairly and lawfully processed
- Processes for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with a person's rights
- Secure
- Not transferred to others without adequate security protection