Coalbrookdale and Ironbridge C.E. Primary School

Policy:

Data Protection Policy

Last Review: Autumn 2017

Responsible: Sue Blackburn

Review Date: Autumn 2019

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 Headteacher and Governors of this 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.

Enquiries

Information about the school's Data Protection Policy is available from the Headteacher. 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

Coalbrookdale & Ironbridge CE Primary School 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 operation 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.

1. The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Responsibilities

The school must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.

The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the Data Controller under the Act.
Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link:

http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff that holds personal information has to comply with the Act when managing that information.
Coalbrookdale & Ironbridge CE Primary School is committed to maintaining the eight principles at all times. This means that the school will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared.
- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- ensure all staff are aware of their responsibilities and of the schools relevant policies and procedures

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

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 Headteacher 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. Pupils' personal data will be checked with parents/guardians at the beginning of each academic year for accuracy.

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 office staff 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 Administrator. 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 (eg 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.

- 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 child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

- Staff data disclosed to relevant authorities eg 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 LA are IT liaison/data processing officers, for example in the LA, 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 which 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

Coalbrookdale & Ironbridge CE 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. Disks, tapes, memory sticks and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school 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 (ie 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. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Headteacher and 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 Headteacher.

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:

The Headteacher
Coalbrookdale & Ironbridge CE Primary School
Dale End
Coalbrookdale
Telford TF8 7DS