BEAL VALE PRIMARY SCHOOL
Learning is for Life, Enjoy the Journey!
Salts Street
Shaw
Oldham,
OL2 7SY
Tel: 0161 770 5752
Email: info@beal-vale.oldham.sch.uk

Data Protection Policy

Data Protection Policy

Policy Statement

Beal Vale Primary School is fully committed to compliance with the requirements of the Data Protection Act 1998.

In order to operate efficiently Beal Vale Primary School has to collect and use personal and sensitive personal data about people with whom it works. These include members of the public (adults & children), current, past, prospective employees, clients and customers and suppliers. In addition it may be required by law to collect, use, share and receive personal and sensitive personal data from the data subject and from third parties in order to comply with the requirements of central government.

This personal and sensitive personal data must be collected, recorded, used, disposed of in accordance with the Data Protection Act 1998 regardless of how the information is held, whether it is on paper, in computer records, audio or visual or any other means. In addition for those working in a social care setting, the Caldicott Principles as laid down by Government must also be followed and demonstrate good practice for all services to follow:

Beal Vale Primary School, as a Data Controller will notify the Information Commissioner the purposes for which it collects personal data. This notification takes place annually and it is a criminal offence not to notify. The Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

Scope

This policy covers all personal and sensitive personal data processed by Beal Vale Primary School and applies to every individual in the Council who has access to personal data about other individuals. In addition it is the school's responsibility to ensure that any non-school individuals who have access to schools processed personal and sensitive personal data comply with the Data Protection Act 1998.

It applies to **all personal and sensitive personal data**

- Processed in the conduct of the school's business, (regardless of, office, mobile or home working).
- Processed in any format, eg, paper, audio, video, electronic, email etc.
- Accessed by schools employees, members, non school personnel
- The school will carefully consider the Data Protection Act 1998 before releasing personal and sensitive personal data about individuals. There are some disclosures of personal and sensitive personal data exempt from the usual restrictions, these disclosures are allowed in specific circumstances, for example, national security, prejudice to prevention and detection of crime or specified regulatory activity. In addition there are circumstances in which the school does not have to disclose information eg,

- There is insufficient identity information of the Data Subject when making a subject access request
- Where the disclosure involves third party information and consent is required
- Health, education and social care information disclosures that may result in serious harm to the data subject or anyone else
- Where it would prejudice the carrying out of social work, prevention and detection of crime, apprehension of offenders, collection of tax or duty.
- Where it would not be in the interests of national security

The Data Protection Principles

The Data Protection Principles are that personal and sensitive personal data

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

2. Shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Shall be accurate and, where necessary, kept up to date

5. Shall not be kept for longer than is necessary for that purpose or those purposes.

6. Shall be processed in accordance with the rights of the data subjects under the Act; and that:

7. Appropriate technical and organizational 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 information shall not be transferred to a county or territory outside of the European Economic Area 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.

Responsibilities

It is the responsibility of every individual to ensure compliance with the Data Protection Act 1998.

All managers are responsible for the application of this policy within their area of responsibility and must ensure that all persons who process, and or have access to personal and sensitive personal data in their area are aware of and understand their responsibilities with regards to the Act. It is noted that some departments have produced their own guidelines and these are to be referred to in conjunction with the corporate documentation.

Any breaches in the compliance with the Data Protection Act 1998 need to be reported to the Information Manager.

The School is obliged under the Data Protection Act 1998 to

- Notify the purposes for which the School processes personal and sensitive personal data
- Adhere to the Data Protection Principles
- Uphold individual rights (data subjects)
- Co-operate with any investigations by the Information Commissioner into alleged breaches of the Data Protection Act 1998 by the Council and comply with any and notices/warrants issued by the Information Commissioner.

Failure to adhere to this policy may lead to breaches of legislation and may lead to Council employees being held liable under the Data Protection Act. In addition the Act makes provisions for the personal liability of Directors for offences by the corporate body that involves the consent and connivance of, or is attributable to any neglect on the part of a person.

Offences include:

- Failure to notify the processing of personal data and any changes to the processing of personal and sensitive personal data
- To unlawfully or recklessly obtain and disclose personal and sensitive personal data
- Offering to sell, selling, personal and sensitive data
- Failure to comply with any notice issued by the Information Commissioner, falsely stating compliance with any notice issued, obstruction of a warrant, and not assisting in the execution of the warrant.

The Caldicott Principles (These reinforce and reflect the data protection principles)

1. Justify the purpose(s)
2. Don't use person-identifiable information unless it is absolutely necessary
3. Use the minimum necessary person-identifiable information
4. Access to person-identifiable information should be on a strict need to know basis
5. Everyone should be aware of their responsibilities
6. Understand and comply with the law

Relationship with existing policies

This policy is relevant to all strategies, policies, procedures, codes, guides etc dealing with information management, personnel, social care, education, information security, Freedom of Information, Environmental Information Regulations, records management and complaints.

Relevant legislation and standards (this list is not exhaustive)

Data Protection Act 1998
Statutory Instruments (various) but including:

- Subject Access Modifications (misc/health/Social Services/Education)
- Processing of sensitive data (elected representatives)

Employment Practices Data Protection codes
EC Directive Data Protection 95/46/EC
Caldicott Guidelines
Human Rights Act 1998
Freedom of Information Act 2000
Environmental Information Regulations 2004
Computer Misuse Act 1990
Taxes Management Act 1970
Regulation of Investigatory Powers Act 2000
Privacy and electronic communications regulations 2003/amendment 2004)
BS IS0 15489 Records Management
BS 7799 Code of practice for information security
FOI Lord Chancellor's code of practice sections 45 on 'Discharge of functions under Part 1' (request handling)
FOI Lord Chancellor's code of practice section 46 (records management)
Local Government Act 1972
Local Government Act (Access to Information) 1985
Public Interest Disclosure Act 1998

Definitions

For the purpose of the Data Protection Policy, and all associated guidance, the definitions are as listed in Appendix I of this Policy.

Policy review and endorsement

This Policy is to be reviewed at intervals no longer than 12 months by the Governing Body.

Appendix I Definitions

Data
There are five types of data:

Computer input documents: eg, forms,
Structured Manual records: eg, files, card indexes, lists, correspondence etc
Automated: eg, computer files, email, telephone logs, images, sounds etc
Accessible records: eg, health, education, social services, housing files etc
*****Unstructured Manual records eg, information not necessarily filed by name, eg, minutes

In fact, as far as public authorities are concerned, the definition of data as extended by the Freedom of Information Act includes All recorded information

***This category is known as Category E data and was introduced into the Data Protection Act by the Freedom of Information Act. In short, this means that any personal information held is potentially accessible. However, if unstructured data is requested then public authorities need not respond unless they are given information to assist them in finding the information. Also, charges can be made for this type of personal information under the FOI charging regime.**

Personal Data*
This is defined as data that relates to a living individual and can be identified directly from that data or indirectly should that data be linked to other data sets. The data encompasses, personal facts, and any expression of opinion or indication of intention to the individual.

Sensitive Personal Data*
This is defined as personal data relating to racial ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental condition, sexual life, allegations or commission of an offence or proceedings relating to an offence**.**

*****The information of deceased persons are not subject to the Data Protection Act 1998 but in these cases access to the information will be looked at on a case by case basis and consider any confidentiality issues arising.

Data Controller
The organization which is responsible for the processing and notification of the processing

Data Subject
Is the individual about whom the personal and sensitive personal data relates

Third Party Information
This can mean information about anyone else and from anyone else other than the data subject, the data controller or data processor.

Processing
Obtaining, recording, holding, carrying our any set of operations on the information or data, including, organizing, adapting, altering, retrieving, consulting, using, transmitting, disseminating, making available, aligning, combining, blocking, erasing or destroying etc etc.