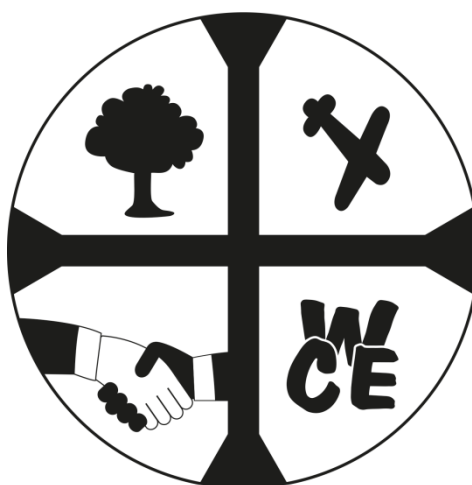


Woodley Church of England (Controlled) Primary School



Name of policy: Data Protection Policy

This policy is due for review on: January 2018

Version	Date Policy Adopted/Reviewed	Approved by governors	Description
1	2009	2009	
2	Reviewed Feb 2012	2012	
3	Reviewed June 2014	2014	
4	To be Reviewed June 2016	2016	

Woodley CE Primary School

Data Protection Policy

General statement

In order to operate efficiently and effectively, the school has to collect and use information about the people with whom it works. This may include members of the public, current, past and prospective employees, clients, customers and suppliers along with past and current pupils.

Scope

This policy applies to all employees, Governors, contractors, agents and representatives and temporary staff working for on behalf of the school.

This policy applies to all personal information created or held by the School in whatever format (eg paper, electronic, email) and however it is stored (for example, ICT systems/databases, shared driving filing structure, email filing cabinet, shelving and personal filing drawers). The DPA (Data Protection Act) does not apply to access to information about deceased individuals.

Responsibilities

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 Head Teacher and Governors of this school intend to fully comply with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All staff involved in the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in line with the DPA.

Requirements

The school commits to following the 8 principles of Data Protection Act. These principles are legally enforceable.

1. Is processed fairly and lawfully
2. Is obtained only for lawful purposes and is not further used in any manner incompatible with those original purposes
3. Is accurate and where necessary is kept up to date

4. Is not kept for longer than is necessary for those purposes
5. Is processed in accordance with the rights of data subjects under the DPA
6. Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss destruction or damage
7. Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.
8. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Notification

The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. The Information Commission maintains a public register of data controllers in which our school is registered.

Privacy Notices

The school commits to being clear and transparent about how personal data is used and to that end, commits to issuing a Fair Processing or Privacy notice to both pupils and staff members once personal information is in its possession. This notice must contain the following information.

- The identity of the data controller eg. The School
- The purpose that the information is being collected or
- Any other purpose that it may be used for
- Who the information will or may be shared with and
- How to contact the Data Controller

This must be at the time that information first starts to be gathered on an individual.

Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. The school should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual to which only s/he is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents, it is important that information regarding one party is not given to the other party to which s/he is not entitled. If speaking to partnering services, such as Social Services, staff should always take a number and call back to confirm identity.

The Individual's right to access their personal information (Subject Access Requests)

Any person whose details are held by the School is entitled under the DPA to ask for a copy of all the information held about them (or child for which they are responsible).

When a request is received, it must be dealt with promptly; a response must be provided as soon as possible and within 40 calendar days and some instances, 15 school days.

The school reserves the right to make a charge to up to the value of £10.00 for this service.

Please also refer to the Freedom of Information Notice for further information on record keeping.

Parents' Rights

An adult with parent responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. This has been judged as being 12 years old. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and the child.

Information Security and storage of data

The school takes information security very seriously and is committed to upholding their responsibilities in this area. We do this by

- Ensuring secure storage of paper records in school.
- Securely backing up any data stored electronically within the European Economic Union
- Ensuring static and portable devices have sufficient encryption and password protection
- Staff taking responsibility for the confidentiality of their passwords and any sensitive data they hold on their school devices. Refer to the Schools Acceptable User Policy and laptop agreement for further conditions of use.
- Comply by the school laptop agreement to ensure laptops are stored safely on and off the premises and information is protected by locking screens when not in use.

It should be borne in mind that at some time in the future the data may be inspected by the courts and a legal official. All data should, therefore, be correct unbiased unambiguous and clearly decipherable and readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Mobile Devices

All mobile devices used in school are subject to the DPA. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The school shall ensure that all devices are secure using encryption and passwords approved by the DPA to maintain data security. Please refer to the BYOD Policy.

Permissions

It is very important to the school that data is only used when permissions have been obtained. Therefore, any person whose details or child's details are to be included in the school website or any photographs of a child which will be published on a variety of media will be required to give

written consent. At the time, full information will be given regarding the use and the scope of the data.

Training

School staff will be informed of the principles of data protection to ensure the highest of standards are maintained and they will be informed of any relevant changes to legislation and subsequent policy reviews and updates.

Breach of the Policy

Non-compliance with the requirements of the DPA by members of staff could lead to serious action being taken by third parties against school authorities. As part of school training, staff will be made aware of the implications on non-compliance.

Policy Review

This Policy will be updated every two years or when changes to best practice or amendments to the Data Protection Act 1998 are made.

Policy adopted – January 2016

Review Date – January 2018