DATA PROTECTION POLICY

Whitehall Infant School

This policy was adopted	**September 2013**
The policy is to be reviewed	**September 2015**
Reviewed by	**Manjit Bringan**

Whitehall Infant School

Data Protection Policy

Whitehall Infant School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Failure to comply with this policy may lead to disciplinary action.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement
The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure our staff are aware of and understand our policies and procedures.

Complaints/Breach
Complaints or breaches of this policy should be referred to the Headteacher.

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts
If you have any enquires in relation to this policy, please contact Mrs M Bringan, Headteacher, who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 5457453.

Appendix 1

Procedures for responding to subject access requests made under the Data Protection Act 1998.

Rights of access to information
There are two distinct rights of access to information held by schools about pupils.
1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2005.

Actioning a subject access request
1. Requests for information must be made in writing; which includes email, and be addressed to Mrs M Bringan, Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.

- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information

Education Pupil Information (England) Regulations 2005.
1. Covers information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body.

2. A request for an educational record must be made in writing and be addressed to Mrs M Bringan, Headteacher and should receive a response within 15 school days.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery.

Complaints
Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Contacts
If you have any queries or concerns regarding these policies / procedures then please contact Mrs M Bringan, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone

Appendix 2

Information Security Guidelines for Schools

The following points are intended to act as a guide for staff to follow when using personal information during the working day and assist in ensuring the school has appropriate security measures in place as required by the Data Protection Act 1998 and the Schools Data Protection Policy.

1. Unauthorised staff and other individuals should be prevented from gaining access to personal information.

2. Visitors should be received and supervised at all times within the school premises, especially where information about individuals is stored.

3. All computer systems containing personal data should be password protected; the level of security will depend on the classification of data being held. You should ensure the Password is of a suitable complexity (A minimum of 8 characters and a mixture of letters and numbers.) Do not share your password with anyone else.

4. Staff should have access to personal information on a "need to know" basis.

5. Computer workstations should not be left signed on when not being used.

6. CDs, disks, tapes, printouts and other storage media containing personal data should be locked away when they are not in use.

7. Only school owned and appropriately encrypted electronic media should be used to store/transport personal data (i.e. laptops, CD Roms, flash drives etc).

8. Be careful about what is sent via email and to whom information is sent. Generally personal data should not be sent in an email unless data can be encrypted or files password protected.

9. The same applies to faxes. If it is absolutely necessary to send personal data via fax then check that the intended recipient of a fax containing personal information is aware that it is being sent in order that they can ensure security on delivery.

10. Ensure that paper files are stored in secure locations and accessed on a "need to know" basis only.

11. When processing personal information do not leave it on public display. All paper files containing personal information should be locked away at the end of each day and not left on desks.

12. Computer monitors should be positioned so that personal data cannot be viewed by anyone not authorised to do so.

13. Security arrangements should form part of a written agreement between the data controller and data processor, if processing is carried out by an external source.

14. Subject to relevant retention periods, redundant personal data should be destroyed by shredding if possible, or by use of an appropriate confidential waste system. If disposable bags are used, they should not be left lying in corridors for collection. CDs, disks, tapes, and other storage media should be either electronically "wiped" or physically destroyed beyond recovery

15. Do not remove personal data (removable media/laptop/file) from school premises unless authorised by the Headteacher. If personal data is to be taken off school premises make sure that it is carried in sturdy lockable bag and is not left unattended at any time. Personal data should not be left in a car overnight and should be stored in a safe location when not in use.