Forty Hill C of E Primary School
Data Protection Policy

This document is a statement of the aims and principles of Forty Hill CE School for ensuring the confidentiality of sensitive information relating to staff, pupils, parents, volunteers and governors.

Introduction
Forty Hill CE Primary School holds a considerable amount of both personal and public data. It is essential that data which is personal remains confidential and data which is public can be made safely available if requested. However, there is sometimes confusion over what is personal and what is public data. The aim of this policy is to provide guidance in this respect. The eight data protection principles are the key to finding that balance and ensuring compliance with the DPA

The Eight Data Protection Act Principles
The act contains eight "Data Protection Principles". These specify that personal data must be:
1. Processed fairly and lawfully.
2. Obtained for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and up to date.
5. Not kept any longer than necessary.
6. Processed in accordance with the "data subject's" (the individual's) rights.
7. Securely kept.
8. Not transferred to any other country without adequate protection in situ.

Practical Considerations
• **Personal data** – we recognise the need to handle personal information in line with the data protection principles
• **Fair processing** – we let pupils and staff know what we do with the personal information you record about them. We make sure we restrict access to personal information to those who need it
• **Security** – we keep confidential information secure when storing it, using it and sharing it with others
• **Disposal** – when disposing of records and equipment, we make sure personal information cannot be retrieved from them
• **Policies** – we have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation
• **Subject access requests** – we recognise, log and monitor subject access requests
• **Data sharing** – where we are legally bound to share personal information, or deem it necessary to achieve our agreed school outcomes, we will take additional reasonable care to ensure data is handled and received securely
• **Websites** – we control access to any restricted area. We make sure we are allowed to publish any personal information (including images) on our website
• **CCTV** – Signage clearly marks where data is being recorded by CCTV and the purpose for which footage is used. CCTV operators comply with all our school policies. CCTV footage is retained securely for fixed periods of time before being deleted. Footage is deemed 'for internal use only'. Only the headteacher can authorise for footage to be released to any other agency.
• **Photographs** – if our school takes photos for publication, we mention our intentions for use
• **Processing by others** –we recognise when others are processing personal information for us and make sure they do it securely
• **Training** – we train staff and governors in the basics of information governance; we recognise where the law and good practice need to be considered; and we know where to turn for further advice
• **Freedom of information** – after consultation, we notify staff what personal information we would provide about them when answering FOI requests.

Definitions
Personal data is information which relates to an identifiable living individual that is processed as data. Processing means: collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.
The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter.

Physical Security and Procedures
We regularly review the physical security of buildings and storage systems, and access to them. This includes storage of paper records and the equipment used to store and process information electronically. Where there is an increased risk of vandalism or burglary, we take these into account.

Electronic Personal Data
Strong passwords, i.e. at least eight characters long and containing special symbols, are used to access any electronic equipment that holds confidential personal information. Some portable devices use encryption software to protect confidential personal information, particularly if they are taken from school premises. Memory sticks should not be used to hold personal information or they should be password protected and fully encrypted.

Use of Private Computer Equipment
If any of the school's personal information is held on private equipment, the school will remain responsible unless it can prove it did everything reasonably possible to keep the information secure.

Paper-Based Personal Data
Whenever possible, storage rooms, strong cabinets, and other storage systems with locks should be used to store paper records. Papers containing confidential personal information should not be left in public view. Particular care should be taken if documents have to be taken out of school.

Disposal of Data
Disposal is a form of processing that needs to be done fairly and in accordance with the seventh principle. "The method of destruction of personal data should take into account the nature of the information. In all cases you must ensure that data is disposed of in a way that creates little risk of an unauthorised third party using it to the data subject's detriment. If any confidential information is held on paper records, they should be shredded or pulped; electronic memories should be scrubbed clean or destroyed"

Policies
The Headteacher has responsibility for raising general data protection awareness and ensuring that policies are adhered to and updated as necessary

Subject Access Requests
Section 7 of the DPA gives individuals the right to request the personal information a school holds about them – the right of subject access. Subject access requests (SARs) are answered within 40 calendar days of receipt. We charge a fee of £10 for answering a SAR. A valid SAR should be in writing – this can include email – and should confirm the requester's identity. We can recognise a subject access request and know who to turn to for detailed advice to ensure compliance with the DPA. We keep a log of the requests that require formal consideration.

Sharing Personal Information
At times we share personal information with other organisations. The main organisations that we share personal data with are:
• Local authorities
• Other schools and educational bodies
• Social services

When sharing information with other organisations, we use secure internal email systems. When we share paper-based confidential personal information, we take every reasonable precaution and action to make sure it reaches the intended recipient.

Freedom of Information Act /Environmental Information Regulations
We have an approved publication scheme and reply to requests for information in line with this legislation. This can be found on the school website.

Accepted by the Governing Body: May 2017
Review Date: May 2020