



***Pattishall Primary is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.***

## **Data Protection Policy**

Pattishall CE Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act 1998.

In paraphrase, the Act is based on eight data protection principles for 'good information handling', which require personal information in that data:

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, kept up to date;
4. is adequate, relevant and not excessive in relation to the purposes for which it is processed;
5. is not kept for longer than is necessary for those purposes;
6. is processed in accordance with the rights of data subjects under the DPA;
7. is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
8. 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.

All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

### **The Data Controller and the Designated Data Controllers**

The School, as a body, is the Data Controller under the 1998 Act, and the Governing Body is therefore ultimately responsible for implementation. However, the Designated Data Controller will deal with day to day matters. The School has identified its Designated Data Controller as The Headteacher. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Headteacher, in the first instance.

### **Responsibilities of Staff**

All staff are responsible for:

- i. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- ii. Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

- iii. Handling all personal data (eg – pupil attainment data) with reference to this policy.

### **Data Security**

1. All staff are responsible for ensuring that:

- i. Any personal data that they hold is kept securely and should not be left in public areas where there is general access.
- ii. Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- iii. Personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) is treated accordingly.
- iv. All portable electronic devices used for storing personal data on school business (including privately owned equipment) should be kept as securely as possible on and off school premises.

2. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

3. Personal information should:

- i. Be kept in a filing cabinet, drawer, or safe in a secure office, or;
- ii. If it is computerised/electronic, be password protected both on a local hard drive and on a network drive that is regularly backed up. If it is sensitive personal data, strong passwords should be used, i.e. at least eight characters long and containing a mixture of letters/symbols/numbers. Passwords should be changed regularly and different passwords used for separate systems and devices.
- iii. If a copy is kept on a usb memory stick or other portable/removable storage media, that media must be password protected, as above, and fully encrypted and/or kept in a secure filing cabinet, drawer, or safe. This is particularly important if they are taken from school premises.

### **Sharing Data**

The school holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing. This information includes contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information.

From time to time, schools are required to pass on some of this data to LAs, the DfE and to agencies that are prescribed by law, such as Ofsted. When considering sharing personal data, staff are responsible for making sure they are allowed to share it; and ensuring that adequate security (taking into account the nature of the information) is in place to protect it.

### **Rights to Access Information**

1. All staff, parents and other users are entitled to:

- i. Know what information the School holds and processes about them or their child and why.
- ii. Know how to gain access to it.
- iii. Know how to keep it up to date.
- iv. Know what the School is doing to comply with its obligations under the 1998 Act.

2. The School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

3. All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The School will ask to see evidence of identity, such as a passport or driving licence, before disclosure of information.

4. The School reserves the right to make a charge to meet the costs of providing the details of the information held.

5. The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

#### **Retention of Data**

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.