

Sutton Benger C of E Aided Primary School

Data Protection Policy (September 2016)

Document Title	Data Protection Policy
Lead Officer	Headteacher & Chair of Governors including Chair of Value for Money Committee; Chair of Teaching and Learning Committee; Chair of Ethos Committee and Chair of Staffing Committee.
Approving Body	Full Governing Body
Edition and Date Approved	Edition 2: 12th September 2016 Version 1
Indicate whether the document is for public access or restricted to internal use only	pdf version to be uploaded to school website.
Summary / Description	This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

DATA PROTECTION POLICY

This policy should be read and understood in conjunction with the following policies and guidance:

- Sutton Benger Primary School Secure Data Handling Policy
- The Data Protection Act 1998 (www.gov.uk)
- Information Sharing: Guidance for Practitioners and Managers HM Govt. Oct 2008
- Information Management Tool Kit for Schools (www.irms.org.uk)

1. Introduction

Sutton Benger Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. In order to accomplish this Sutton Benger Primary School must comply with the Data Protection Principles (**'Principles'**) which are set out in the Data protection Act 1988 (the **'1998 Act'**).

In summary these Principles state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specific and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and up to date.
- Not be kept for longer than is necessary for the purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorized access, accidental loss or destruction.

Sutton Benger Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times.

2. Status of this Policy

This policy does not form part of the contract or 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.

3. The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has four Designated Data Controllers:

- Executive Headteacher (Primary)
- Associate Headteacher (Primary)
- Office Administrators
- Finance Officer

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about themselves or their child should raise the matter with the Executive and/or Associate Headteacher.

4. Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they provided e.g. change of address

The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupils course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the Schools Data Protection Conditions as set out in Section 5 below.

5. Schools Data Protection Conditions

- a. The 1998 Data Protection Act extends data protection law to cover personal data held in manual systems as well as on computer. It places strict conditions on the processing of 'sensitive' personal data and strengthens individual rights (including enhanced right of access to personal data). The School has an obligation to apply rigorous standards when processing information and commits itself to ensuring that both the word and spirit of the Data Protection legislation is adhered to.**

b. The Act is underpinned by eight Data Protection Principles (Schedule 1). These principles state that personal data shall:

1. be processed fairly and lawfully, and in particular, shall not be processed unless:
 - (i) at least one of the conditions in Schedule 2 of the Act is met;
 - (ii) in the case of sensitive personnel data, at least one of the conditions in Schedule 3 of the Act is also met.
2. 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. be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. be accurate and kept up to date.
5. be kept for no longer than is necessary for that purpose or those purposes.
6. be processed in accordance with the rights of data subjects under the Act.
7. not be transferred to a country or territory outside 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.

and that:
8. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personnel data and against accidental loss or destruction of, or damage to, personal data.

c. The School will, through appropriate management, apply a strict application of criteria and controls. The School will:

1. observe fully the conditions regarding the fair collection and use of information.
2. meet its legal obligations to specify the purpose for which information is used.
3. collect and process information only to the extent that it is required to meet operational needs or to comply with any legal requirements.
4. ensure the quality of information used.
5. apply strict checks to determine the length of time the information is held.
6. ensure that the rights of people about whom information is held can be fully exercised under the Act. These include the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances, and the right to correct and rectify, block or erase information which is regarded as wrong information.

7. observe and implement fully the conditions for processing 'Sensitive Personal Data' as defined in Schedule 2 of the Act. (See Glossary for the definition of Sensitive Personal Data.) Sutton Benger C of E Aided Primary School will ensure that the conditions of Schedules 2 and 3 of the Act are adhered to when processing such data.
8. all forms and documentation which are used for the collection of personal data are to include the following DPA1998 or similar statement:

'Sutton Benger C of E Aided Primary School has a duty to protect personal information; Sutton Benger C of E Aided Primary School will process this information in accordance with the Data Protection Act 1998. This information will be stored on computer and in manual files'
9. take appropriate technical and organisational security measures to safeguard personal information. Such measures will be in accordance with the requirements of BS7799 Parts 1 and 2 Information Security Management.
10. give clear guidelines on how to dispose of data held both electronically and on paper records.
11. ensure that personal information is not transferred abroad without suitable safeguards.

d. In addition Sutton Benger C of E Aided Primary School will ensure:

1. that someone is appointed with specific responsibility for data protection within the School. The nominated person is the Executive Headteacher.
2. in the absence of the Data Protection Officer (DPO), a deputy representative for the School is appointed. The nominated person is the Associate Headteacher.
3. the DPO is to ensure that the School is compliant with the requirements of the Data Protection Act 1998. She is to be supported by the Full Governing Body in order to carry out her duties and responsibilities. In addition the DPO is to ensure that:
 - i. all School personnel are given adequate training in Data Protection.
 - ii. all requests from data subjects are processed initially through the DPO.
 - iii. all the data subject access requests are handled in accordance with the School's Data Subject Access procedures. All subject access requests are to be centrally controlled by the DPO, who is to ensure that all requests are handled within 40 days.
 - iv. Data Controllers are briefed and are provided with guidance pertaining to their duties.
4. notifications of IT systems and manual files holding personal data are registered with the Information Commissioner.

5. that the DPO maintains a central register of all notifications and all notifications are made by the DPO.
6. everyone employed by Sutton Benger C of E V o l u n t a r y Aided Primary School and managing personal information understands that they are contractually responsible for following good data protection practice.
7. that any agency operating on behalf of Sutton Benger C of E V o l u n t a r y Aided Primary School (the data controller) as a data processor is able to maintain adequate security in accordance with the requirements of principal 7 of the Act and is committed to do so under contract.
8. everyone managing and handling personal information is appropriately trained to do so.
9. everyone managing and handling personal information is appropriately supervised.
10. data protection requirements are included in all third party contracts.
11. queries about handling personal information are promptly and courteously dealt with.
12. hardcopy data consigned for destruction is disposed of as follows:
 - i. personal sensitive data – shredded
 - ii. non sensitive personal data – normal waste disposal
13. that methods of handling personal information are clearly described and procedures are provided for all data controllers of personnel information.
14. a regular review and audit is made of the way personal information is managed. Data controllers are to review the retention periods for their data.
15. methods of handling personal information are regularly assessed and evaluated.
16. performance with handling personal information is regularly assessed and evaluated
17. procedures confirming the reliability of employees / contractors / agencies who have access to personal / sensitive data are checked for reliability.
18. notifications are kept up to date with the Information Commissioner's Office and are subject to an annual review.
19. any recommendations derived from the review will be acted upon where appropriate.

6. Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via the Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

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

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerized, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

7. Rights to Access Information

All staff, parents and other users are entitled to:

1. Know what information the School holds and processes about them or their child and why.
2. Know how to gain access to it.
3. Know how to keep it up to date.
4. Know what the School is doing to comply with its obligations under the 1998 Act.

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 types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1988 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 complete the '*Access to Personal Data Request Form*' and submit to the Executive Headteacher.

The School will make a charge of £10 on each occasion that access is requested, although the School has discretion to waive this fee.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided with forty (40) calendar days, as required by the 1988 Act.

8. Subject Consent

In many cases, the School can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined under the 1988 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other legislation to ensure that staff are suitable for the job.

The School has a duty of care to all staff and children and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users.

The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process data in the event of a medical emergency.

9. Processing Sensitive information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick pay Policy or the Equal Opportunities Policy.

Because the information is considered 'sensitive' under the 1988 Act, staff (and pupils where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

10. Publication of School information

Certain items of information relating to the School staff will be made available via searchable directories on the public website, in order to meet legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

11. 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 or academic transcripts.

Retention periods for data will vary depending on the nature of the information.

12. Conclusion

Compliance with the 1988 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

GLOSSARY

Act	The Data Protection Act 1998.
Accessible Records	Health records created by a health professional, a school education record or public record relevant to local authority housing or social services.
Archive	The documents created or received and accumulated by a person or organisation in the course of the conduct of affairs, and preserved because of their continuing value.
BS	British Standard
Data	Information which is: <ul style="list-style-type: none">a. being processed by means of equipment operating automatically in response to instructions given for that purposeb. recorded with the intention that it should be processed by means of such equipmentc. recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing systemd. written, printed in electronic form, taped, photographed or in other media. It includes microfilm, movie film, CCTV videotape, etc. or, information which: <ul style="list-style-type: none">e. does not fall within paragraphs a, b or c, but forms part of an accessible record as defined by Section 68 of the Act.
Data Controller	Person who (either alone, jointly or in common with other persons) determines the purpose for which, or the manner in which, any personal data is, or is to be, processed.
Data Protection Officer (DPO)	Person within the organisation appointed to oversee all aspects of the implementation of the Act within the organisation.
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Protection Principles	The principles that determine what data can be processed, collected or stored. Failure to abide by the Principles is a breach of the Act.
Data Subject	The individual who is the subject of the personal data.

European Economic Area (' E E A ')

This comprises all the member states of the European Union plus some other countries with associate status. The current members of the EEA are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

Notification

Informing the Commissioner that an organisation or individual will be processing data other than for private or other exempted uses.

Personal Data

Data that relates to a 'living individual' who can be identified:

- a. from the data
- b. from the data which is in the possession of, or is likely to come into the possession of, the data controller
- c. includes an expression of opinion about the individual, and indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Data Personal data which consists of the following information:

- a. the racial or ethnic origin of the data subject
- b. his/her political opinions
- c. his/her religious beliefs or other beliefs of a similar nature
- d. whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- e. his/her mental health or conditions
- f. his/her sexual life
- g. the commission or alleged commission of any offence
- h. any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceeding or the sentence of any court in such proceedings.

Special Purposes

Term used to denote certain types of activity that are subject to particular rules under the Act. This means any one or more of the purpose of journalism, artistic purposes and literary purposes.

Subject Consent

Before processing personal data, the data controller may have to have the agreement of the individual to do so.

Third Party

Any person other than:

- a. Data Subject
- b. Data Controller
- c. Data Processor