



<b>Data Protection Policy (including Protection of children’s biometric information)</b>	
Date	November 21
Review	November 23
Reviewed by	Data Protection Officer Mrs Kerridge and reviewed by resources committee every two years
Statutory Policy for Website	
<b>Related Policy and Information:</b>	
<ul style="list-style-type: none"> <li>• Governors and Volunteers privacy notice</li> <li>• Job applicants Privacy notice</li> <li>• Use of Parents and Carers Data</li> <li>• School’s Work force privacy notice</li> <li>• For parents and cares use of their child’s data privacy notice</li> </ul>	

Sandlings Primary 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 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. These details are then available on the ICO’s website. Schools also have a duty to issue a Data Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

**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.

## **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 and 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 is 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

## **Biometric recognition systems**

Currently our school does not use any biometrical recognition systems where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash which would need to comply with the requirements of the Protection of Freedoms Act 2012).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Currently we do not use any systems for staff but if new systems were introduced we would also obtain their consent before they first take part in it, and provide alternative means of accessing the

relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

### **Data Breach**

In the event of a data breach the schools Data Breach Procedures will be followed. The Data Protection Officer will contact the ICO. Online at <https://ico.org.uk/concerns/> or by telephone on 0303 123 1113, in accordance with the Schools Data Protection Policy.

### **Complaints**

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

### **Review**

This policy will be reviewed as it is deemed appropriate, but not less frequently than every year. The policy review will be undertaken by the Headteacher and the Resources Committee.

### **Contacts**

If you have any enquires in relation to this policy, please contact the school office, on 01394 420444 or by email [admin@sandlings.suffolk.sch.uk](mailto:admin@sandlings.suffolk.sch.uk) who will also act as the contact point for any subject access requests. The details of the information held by the school and subject access requests can be found in Appendix 1.

Further advice and information is available from the Information Commissioner's Office, [www.ico.gov.uk](http://www.ico.gov.uk) or telephone 0303 123 1113

## **Appendix 1**

### **Sandlings Primary School**

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 (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

#### **Actioning a subject access request**

1. Requests for information must be made in writing; which includes email, and be addressed to [admin@sandlings.suffolk.sch.uk](mailto:admin@sandlings.suffolk.sch.uk) 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 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; **therefore, all information will be reviewed prior to disclosure.**

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed,

nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. 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. If postal systems have to be used, then registered/recorded mail must be used.

### **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.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

### **Contacts**

If you have any queries or concerns regarding these policies / procedures, then please contact the school office.

Further advice and information can be obtained from the Information Commissioner's Office, [www.ico.gov.uk](http://www.ico.gov.uk) or telephone 0303 123 1113