St.Nicholas School

DATA PROTECTION AND INFORMATION MANAGEMENT

St Nicholas School is working towards the UNICEF Rights Respecting School Award and promotes rights respecting values in all its policies

The Governing Body of St Nicholas School reviewed

this Policy on

It will be reviewed in annually unless advised by Croydon LA

Signed _____Headteacher date_____

Signed _____Chair of Governors date_____

Contents:

Statement of intent

St Nicholas School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 1998.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the Act:

- Data must be processed fairly and lawfully.
- Data must only be acquired for one or more lawful purposes and should not be processed for other reasons.
- Data must be adequate, relevant and not excessive.
- Data must be kept accurate and up-to-date.
- Data must not be kept for longer than is necessary.
- Data must be processed in accordance with the data subject's rights.
- Appropriate measures must be taken to prevent unauthorised or unlawful access to data and against loss, destruction or damage to data.
- Data must not be transferred to a country or territory unless it ensures an adequate level of protection for the rights of the subject.

Organisational methods for keeping data secure are imperative, and **St Nicholas School** believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2013)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will be implemented in conjunction with the school's:

- Photographs in School Policy.
- E-security Policy.
- Freedom of Information Policy.
- CCTV Policy.

2. Data controller

2.1. **St Nicholas School**, as the corporate body, is the data controller.

2.2. The **governing body** of **St Nicholas School** therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

2.3. The **School business manager** deals with the day-to-day matters relating to data protection.

2.4. The **school business manager** is responsible for processing personal information on the school's behalf. The security of the personal information is covered in a written agreement between the school and the **school business manager**.

2.5. On occasion, personal information may be processed by outside organisations involved in data processing. By involving another organisation in data processing, the school increases certain risks. The security of the personal information is covered in a formal contract between the school and any outside organisation.

3. Fair processing

3.1. **St Nicholas School** recognises that its staff and pupils need to know what the school does with the information it holds about them.

3.2. Parents/carers receive a copy of this Data Protection Policy upon registration of their child at the school, as well as an overview of the information that the school will keep about their child.

3.3. **St Nicholas School** issues a general privacy notice, detailing the purposes for which personal data collected by the school will be used.

3.4. If personal details are being recorded for a specific purpose, a specific privacy notice is issued.

3.5. The general privacy notice is also published on the school's website.

3.6. Personal information is only made available to staff and governors who need that particular information to do their jobs, and is only made available at the time that it is needed.

3.7. All members of staff, including members of the governing body, receive training in their responsibilities under the Data Protection Act, and guidance on confidentiality of personal information, as part of their induction.

3.8. The training is reinforced at regular intervals throughout their employment or term as governor.

3.9. Members of staff and parents/carers are responsible for checking that any information that they provide to the school, in connection with their employment or in regard to a registered pupil, is accurate and up-to-date.

3.10. **St Nicholas School** cannot be held accountable for any errors unless the employee or parent has informed the school about such changes.

3.11. The **school business manager** is responsible for monitoring fair processing controls on an on-going basis.

4. Data security

4.1. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

4.2. Confidential paper records are not left unattended or in clear view anywhere with general access.

4.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

4.4. Where data is saved on removable storage or a portable device, the device is kept in a locked filing cabinet, drawer or safe when not in use.

4.5. Memory sticks are not used to hold personal information unless they are password-protected and fully encrypted.

4.6. All electronic devices are password-protected to protect the information on the device in case of theft.

4.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

4.8. Staff and governors do not use their personal laptops or computers for school purposes.

4.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

4.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

4.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

4.12. When sending confidential information by fax, staff always check that the recipient is correct before sending.

4.13. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

4.14. Before sharing data, all staff always ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

4.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

4.16. The physical security of the school's buildings and storage systems, and access to them, is reviewed **termly**. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

4.17. **St Nicholas School** takes its duties under the Data Protection Act seriously and any unauthorised disclosure may result in disciplinary action.

4.18. The **school business manager** is responsible for continuity and recovery measures are in place to ensure the security of protected data.

5. Subject consent

5.1. **St Nicholas School** understands that subjects have certain legal rights to their personal data, which will be respected.

5.2. The school does not process personal data without the consent of the subject, although the processing of data will sometimes be necessary for:

- The performance of a contract to which the subject is party to, or the steps taken with a view to entering a contract.
- Compliance with a legal obligation to which the school is subject.
- The administration of justice, legal functions of persons or departments, or functions of a public nature exercised in the public interest.
- The purposes of legitimate interests of the school, unless the decision prejudices the rights, freedoms or legitimate interests of the subject.

5.3. Members of staff will be working in close contact with children. Disclosure and Barring Service (DBS) checks will therefore be made a condition of employment in order to ensure that potential employees do not pose a threat or danger.

5.4. Sensitive data, including: information relating to a subject's racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health; their sex life; or the commission of any offence, can only be processed with the explicit consent of the subject.

5.5. Sensitive data is processed if it meets the following requirements:

- It is necessary to protect the subject's vital interests
- It is carried out in the course of legitimate activities by a not-for-profit body or association with appropriate safeguard
- It is necessary for the administration of justice or other legal purposes
- It has been ordered by the Secretary of State
- It is necessary to prevent fraud
- It is necessary for medical purposes
- It is necessary for equality reasons
- It was made public deliberately by the data subject

6. Rights to access information

6.1. All members of staff, parents/carers of registered pupils and other users are entitled to:

- Know what information the school holds and processes about them or their child, and why.
- Understand how to gain access to it.
- Understand how to keep it up-to-date.
- Understand what the school is doing to comply with its obligations under the Data Protection Act.

6.2. All members of staff, parents/carers of registered pupils and other users have the right, under the Data Protection Act, to access certain personal data being held about them or their child.

6.3. Personal information can be shared with pupils once they are old enough, although this information can still be shared with parents/carers.

6.4. Pupils who are old enough to make decisions for themselves, are entitled to have their personal information handled in accordance with their rights.

6.5. **St Nicholas School** complies with requests for access to personal information as quickly as possible, but will ensure that it meets its duty under the Data Protection Act to provide it within 40 working days.

6.6. **St Nicholas School** complies with its obligations under the Data Protection Act to provide subjects access to personal information.

6.7. All subject access requests are kept in a log that requires formal consideration.

6.8. The school may charge a fee of £10 or more on each occasion that access is requested.

6.9. **St Nicholas School** is not obliged to provide unstructured personal data if the administrative cost is deemed to exceed the limit of £450 as contained in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

6.10. **St Nicholas School** is not obliged to supply access to information unless it has received:

- A request in writing.
- The fee required.

7. Publication of information

7.1. **St Nicholas School** publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures.
- Minutes of meetings.
- Annual reports.
- Financial information.

7.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

7.3. **St Nicholas School** does not publish any personal information, including photos, on its website without the permission of the affected individual.

7.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

8. CCTV and photography

8.1. **St Nicholas School** understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.

8.2. **St Nicholas School** notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

8.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

8.4. **St Nicholas School** keeps CCTV footage for **six months** for security purposes; the **school business manager** is responsible for keeping the records secure and allowing access.

8.5. The school always indicates its intentions for taking photographs of pupils and retrieves permission before publishing them.

8.6. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission is sought for the particular usage from the parent/carer of the pupil.

8.7. Precautions, as outlined in the Photography Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

8.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the Data Protection Act.

9. Data retention

9.1. The Data Protection Act states that data should not be kept for longer than is necessary.

9.2. In the case of **St Nicholas School**, unrequired data is deleted as soon as practicable.

9.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

9.4. Paper documents are shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

10. DBS data

10.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

10.2. Data provided by the DBS is never duplicated.

10.3. Any third parties who access DBS information are made aware of the data protection legislation, as well as their responsibilities as a data handler.

11. Challenges and compensation

11.1. **St Nicholas School** understands that members of staff and the parents/carers of registered pupils have the right to prevent the processing of personal data if it is likely to cause damage or distress.

11.2. Individuals with concerns related to the processing of personal data should provide the **school business manager** with written notice.

11.3. If the **school business manager** receives a written notice asking them to cease or not to begin processing specified data, they attempt to reply in writing within 21 days detailing:

- Their compliance or their intent to comply.
- Their reasons for considering the subject's written notice unjustified and the extent to which they have complied, or intend to comply, with the request.

11.4. Data subjects reserve the right to take their concerns to a court of law and will be entitled to compensation if it is judged that the school contravened the provisions of the Data Protection Act.

11.5. Individuals who are not the subject of the data, but suffer damage as a result of the contravention, are also entitled to compensation.

11.6. It is the individual's own responsibility to take action for compensation if loss of personal data causes them damage.

11.7. The school will immediately rectify, block, erase or destroy any data that a court of law judges to have contravened the requirements of the Data Protection Act.

12. Policy review

12.1. This policy is reviewed every **two years** by the **school business manager** and the **headteacher**.

12.2. The scheduled review date for this policy is **October 2018**.