# SAINT NICHOLAS SCHOOL

# DATA PROTECTION POLICY

***Note: This policy applies to all sections of the school including EYFS***

Last review: September 2013

Next review: November 2016

## 1. INTRODUCTION

The school aims to process all its children's and employees' records in accordance with the Data Protection Act 1998. Under this Act, individuals have certain rights of access to data which is held on them in either manual or electronic form. The school aims not to store any information, opinion or judgement that could not be shown to its subject and explained or justified if necessary.

## 2. EMPLOYEES

Subject to the following provisions, employees will have the right of open access to their personal employment records.

### 2.1 Scope

A *personal employment record* is a manual and/or electronic record, and their contents, which is capable of enabling the identification of the particular employee by way of a personal identifier, including:

- any record the contents of which relate exclusively to a named employee and which is held in the Bursar's office, and which would be regarded, in whole or in part, as being the *'personnel record';*
- any record the contents of which relate exclusively to a named employee and which is held in the Accounts Office, and which would be regarded, in whole or in part, as being the *'payroll record';*
- any similar or equivalent record.

### 2.2 Contents

A personal employment record may contain any information legitimately required for the purposes of:

- statutory employment records
- operational management and administration.
- These may include, *inter alia*:
- applications for vacancies and CVs
- interview records
- confidential references
- medical reports
- offers of employment
- statutory statements of terms and conditions
- disciplinary and grievance records
- performance appraisals and similar reviews
- notes of informal meetings and interviews
- training details
- salary details
- related correspondence
- attendance records.

These are examples only and there may be other legitimate entries that are included. Any data or other material that cannot legitimately be shown to be related directly or indirectly to the employment of the employee concerned is not included. All records (be it in hard copy or electronic form) are kept in a secure location with controlled access for those that are authorised to have access.

## 2.3 Sensitive personal data

The 1998 Data Protection Act defines *sensitive personal data* as personal data which relates to:

- racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of a similar nature
- whether he or she is a member of a trade union
- physical or mental health or condition
- sexual life
- the commission or alleged commission of any offence
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Act prohibits the processing of sensitive data except in specified circumstances, for example ethnic monitoring.

## 2.4 Employee rights

Employees will have right of access to their personal employment record normally within five working days of written notice being received by the Head. In response to a request, the Head will confirm the date, time and place at which access will be provided and will confirm the access fee that will be charged.

Access will be by arrangement and viewing of the contents of the record will be at its kept location in the presence of a person nominated by the Head. The purpose of this provision is solely for the purposes of ensuring that no material is inappropriately removed or destroyed.

Employees may, within reason, request one copy of any or all of the contents of a record if they wish. A record will be made of any copies requested and where possible provided, including date and place together with the name of the person providing them.

An employee may challenge the accuracy of an entry in the record and where, on investigation, it is found to be inaccurate shall be entitled to have the entry corrected or removed, whichever is the most appropriate, and to have this action confirmed in writing as having been done.

An employee may challenge the legitimacy of making or keeping particular data or other information in the record.

## 2.5 Confidential references

Confidential references given by the school are exempt from subject access under the Data Protection Act. References requested and received by the school from other employers are provided in confidence. Employees will be entitled to have access to references received should they so request only if the provider of the reference has consented and there is no other substantial reason for the school to do otherwise.

# 3. CHILDREN

The school will maintain records and obtain and share information (with parents and carers, other professionals working with the child, and the police, social services and Ofsted as appropriate) to ensure the safe and efficient management of the setting, and to help ensure the needs of all children are met.

## 3.1 Confidential information and records

Children's confidential information and records (be it in hard copy or electronic form) are easily accessible and available. These records are only accessible and available to those who have a right or professional need to see

them. In line with our Safeguarding & Child Protection Policy we reserve the right to share confidential information on a need to know basis with other professionals in order to meet the individual needs of the child.

### Paper records & confidential information

Paper records are stored securely in locked filing cabinets in a locked room adjacent to the Heads' office in Hillingdon House.

### Electronic records & confidential information

Electronic records and confidential information are stored on the school's secured database, Engage. This data is backed up daily. Information stored on our computers is protected by industry standard software.

## 3.2 Data Protection Act (DPA) 1998 & the Freedom of Information Act 2000

The school are aware of their responsibilities under the Data Protection Act (DPA) 1998 and where relevant the Freedom of Information Act 2000.

## 3.3 Privacy of the children

The school will ensure that all staff understand the need to protect the privacy of the children in their care as well the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality.

## 3.4 Parents and/or carers access to records & information

The school will enable a regular two-way flow of information with parents and/or carers, and between providers, if a child is attending more than one setting.

Parents and/or carers will be given access to all records about their child, provided that no relevant exemptions apply to their disclosure under the DPA.

If requested, the school will incorporate parents' and/or carers' comments into children's records.

## 3.5 Retention of records

Records relating to individual children must be retained for a reasonable period of time after they have left the provision.

# 4. DATA SECURITY

Staff: All staff are responsible for ensuring that:

(i) Any personal data on pupils [or staff], to which they have access, or for which they are responsible, is kept securely, for example:

- Kept in a locked filing cabinet; or
- In a locked drawer;
- If it is computerised, be password protected.
- If computerised, that the computer itself is kept in suitably secure conditions. Data should not be stored on the hard drives of desktop personal computers but on the networked storage facilities provided.

(ii) Permission to store information on laptop computers (or off-site) must be:

- obtained in writing from the Head;
- the computer must at all times be maintained physically secure e.g. locked into the boot of a car when travelling or in a locked house / dwelling at other times or retained by the user when using public transport;
- where the data is particularly sensitive, a two form security factor must be used e.g. RSA dongle. This would protect the information in the event of the loss or theft of the computer;
- Care must be taken to ensure that data is frequently transferred to network storage and that discrepancies are not allowed to arise;

- Where information is to be gathered through, or used on, a website, then appropriate measures must be in place to control access and prevent unauthorised disclosure.

(iii) Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

(iv) Advice on the collection, retention and secure storage of information may be obtained from the Head.

(v) Staff should note that unauthorised disclosure is a breach of the Data Protection Act and lSO result in a personal liability for the individual staff member.

## 5. COMPLAINTS

Complaints will be dealt with in accordance with the school's complaints policy.

## 6. COMMITMENT

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why personal information is being collected.
- Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
- Ensure all staff and governors are aware of and understand these policies and procedures.