

St John Baptist (Southend) CE Primary School

RECORDS MANGEMENT POLICY

Agreed: December 2015

Signed by Chair: Andrea Blower

Review Date: November 2017

Records Management Policy

Purpose of Policy

St John Baptist School has a responsibility to protect the personal and sensitive information which is collected from parents, children and staff and governors. Our school needs to make sure that we are collecting, processing, holding, storing and transporting personal and sensitive data in accordance with the Data Protection Act 1998.

This policy provides a clear and concise framework for the management of the schools records.

Policy Contents

1. Collection of data
2. Accuracy of data
3. Security of paper records/documents outside of school premises
4. Sending information by post
5. Version Control of data
6. Clear Desk and Screen
7. Secure Disposal of Records & Schools Retention Schedule
8. Sharing data with third parties
9. Responsibilities
10. What happens if this policy is breached
11. Review
12. Policy Authorisation and Control

APPENDIX 1- Fair Processing template

1. Collection of data

The Data Protection Act requires all data controllers to collect and process personal and sensitive data fairly and lawfully.

When collecting personal and/or sensitive data from individuals it is important that they understand what their data is being collected for. This will be covered by providing the parents/guardians with the school's privacy notice when a child starts at the school and using fair processing notices when collecting data on forms (paper or electronic). See Appendix 1 for the Fair Processing template.

Our Fair Processing Notice will inform individuals what their data will be used for and must give any extra information the school think they need to know to enable St John's to process their information fairly.

When using a Fair Processing Notice on a form, it is best placed above the dated signatory section.

Some personal and/or sensitive data will be collected throughout a pupil or member of staff time at the school. This data must be kept securely protected at all times and can be subject to any 'Access to Information' requests.

It is against the law to unlawfully obtain, use and sell personal and/or sensitive data under the Data Protection Act.

2. Accuracy of data

Is it important to have an accurate and up to date record of next of kin details/contact details therefore this data must be updated on an annual basis. If this data becomes inaccurate a child could be put at risk.

It is important to have an accurate and up to date record of next of kin details/contact details for member of staff too in case of an emergency. These must also be reviewed on an annual basis or when there is a change in staff.

3. Security of paper records/documents outside of school premises

Paper which contains personal sensitive data must only be taken off school premises if that data is not accessible via an encrypted device. When paper records/documents are taken off site they must be kept to a minimum and a register of the data that is in use must be kept at the school. When the data is returned back to the school it must be signed in. This creates a concise audit trail to avoid data not being returned and no one realising data is missing.

Paper documents which contain personal sensitive data must be transported from one location to another in a lockable bag provided at the school office.

4. Sending information by post

The loss of paper records which contain personal/sensitive data could lead to a serious breach. A serious data breach requires St John Baptist School to notify the Information Commissioner's Office and this could lead to a monetary penalty being levied.

St John's will not rely on standard postal services when sending personal, sensitive or confidential information if there would be significant impact on its loss. St John's will reduce the risk by looking at alternative delivery methods:

- Use recorded or special delivery post
- Use a reliable courier service
- Consider secure e-mail or encrypted media if possible

When sending personal, sensitive, or confidential information by post check to ensure the correct information is being sent to the correct recipient.

5. Version Control of data

It is important that electronic records are available as unique documents to avoid multiple versions of data which can become out of date.

Therefore it is important that:

- Access control is monitored and updated on a regular basis
- All documents are accessible to staff who needs to see them and one version is available to all
- Data is easy to locate for access to information requests

6. Clear Desk and Screen

It is important to keep the working environment clean and tidy in order to practice good records management. Take time to do the following tasks:

- Clear out desk drawers and cupboards on a planned basis.
- Use the cross cut shredder provided in the school office to dispose of confidential office paper when it is no longer needed.
- Do not print off confidential e-mails to read as this will generate extra paper and extra risk.
- If you print confidential information collect it from the printer immediately
- If you see confidential data left on the printer and you are the last person to leave the office at the end of the day, shred the documents before you leave or lock them away.
- When sending a fax ensure you send it to the correct fax number and then call the recipient to make sure they have received it.
- Do not leave confidential information out on your desk when you are away from it. Lock away confidential information if you are on a break and at the end of each working day.
- Aim to handle any piece of paper containing personal/sensitive data once. When you have read it and are finished with it, either file it away or shred it.
- Be sure to double check any paper documentation you put in envelopes to go out in the post. This will avoid individuals being sent confidential information which doesn't belong to them.
- Do not leave confidential data visible on your computer screen when your computer is not in use. Make sure systems, documents, etc are shut down and not accessible if you leave your desk for a break.
- Staff pigeon holes must not be used as a filing cabinet, therefore they must be checked and cleared out daily to avoid confidential data being compromised.

7. Secure Disposal of Records & Schools Retention Schedule

St John Baptist School has a current and up to date retention schedule which sets out how long personal and/or sensitive data must be held for in line with the Data Protection Act.

Personal and/or sensitive data must be destroyed in line with the school's retention schedule which can be requested from the Head of School. It is of the utmost importance to work to the schedule and not keep data longer than necessary.

All data destroyed must be logged and recorded on the school records of destruction spreadsheet which creates an audit trail for documentation that no longer needs to be retained by law.

If St John Baptist School has any unwanted ICT equipment that is no longer in use and needs to be securely disposed of, contact the schools data protection officer to arrange secure disposal through the Local Authorities ICEX contract.

8. Sharing data with third parties

When St John Baptist School shares personal and/or sensitive data with third party providers there must be sufficient data-sharing protocols in place. This can be recorded in a contract, within a confidentiality statement or an Information Sharing Agreement.

If staff become aware that data personal and/or sensitive data is going to be shared outside of the school, call the school's Data Protection Advisor for advice and guidance.

9. Responsibilities

All information collected, and records created by St John Baptist School are the property of the school, not any individual, and must not be used for any activity or purpose other than the school's official business.

Head of School

- Advising school staff on records management, policy and procedures.

School Business Manager

- Ensuring that the management of schools records is kept up to date with regular checks.
- Implementing the Records Management policy.
- Maintaining the schools retention schedules.

All Staff

- Have a responsibility to abide by the Records Management policy. Any breach of this policy could lead to disciplinary action being taken.

St John Baptist School senior staff will meet with the school's Data Protection Officer on a quarterly basis where any records management tasks, ideas & issues will be discussed.

The Data Protection Officer will provide advice and guidance to the school as and when needed and is available to answer questions from 9am-5pm Monday to Friday on **07580 750 757** or **0208 314 9642/0208 314 9928** or e-mail Schoolsdpa@lewisham.gov.uk.

10. What happens if this policy is breached

Failure to adhere to this or any related policy, could lead to disciplinary action.

11. Review

This policy will be reviewed November 2017.

12. Policy Authorisation and Control

Role	Name	Version	Date
DP Officer for Schools	Zoe Horsewell	V1.1 first draft	20/11/15
Head of School	Caroline Phillips	V1.1 first draft	20/11/15
Business Manager	Joyce Joseph	V1.1 first draft	20/11/15
Chair of Governors	Andrea Blower	V1.1 first draft	20/11/15

Fair Processing Notice Template
'Why and how we collect and use your data'

The Data Protection Act 1998

For the purposes of the Data Protection Act 1998, St John Baptist School is the data controller and therefore is responsible for the information it collects.

The information on this form is being collected

.....
.....
.....
.....

The information on this form will not be shared with any third parties without your consent unless in exceptional circumstances, such as when we are required to by law. We will keep all information safe and secure.

OR

The information on this form will also be shared with (name third parties and explain why it will be shared) and also in exceptional circumstances, such as when we are required to by law. We will keep all information safe and secure.

For more information on how St John Baptist School handles your data please see the school's privacy notice which is available at the school office.