RUSHEY GREEN PRIMARY SCHOOL

RECORDS MANAGEMENT POLICY

Reviewed by: Resources Committee **Date:** 23rd. April 2019 **Signed:**

Last reviewed on: April 2018

Next review due by: September 2022

Purpose of Policy

Rushey Green Primary School has a responsibility to protect the personal and sensitive information that we hold from parents, children and staff. This information requires careful management and our school needs to make sure that we are collecting, processing, holding, storing and transporting personal and sensitive data in accordance with the General Data Protection Regulation 2016.

This policy sets out the school's responsibilities and provides a clear and concise framework for the management of the schools records. The aim of this policy is to ensure that the school:

- Collects accurate, authentic and reliable data
- Maintains records to meet the school's business needs
- Disposes of data that is no longer required in an appropriate manner
- Protects vital records
- Conforms to any legal and statutory requirements relating to record-keeping for the retention and destruction of records
- Complies with government directives and with the General Data Protection Regulation 2016 to protect the data it holds.

1. Introduction

School recognises that its records are a vital business resource and are key to the effective functioning and accountability of the school. Efficient management of records is essential in order to:

- Support the Schools core business activities
- Comply with legal and statutory requirements
- Provide a high quality service to our children, parents, guardians/carers and members of staff

This policy provides a framework for the management of School's

records. **Objectives**

The policy covers all records created and received by the School, in any format. A record is defined as a document held in any format including but not limited to: paper documents, audio recordings and electronic data for example:

- Applications and any other forms
- Staff notes relating to the school work
- Word-processed correspondence, minutes of meetings, policies, strategies and other documents;
- plans, drawings and photographs, whether analogue or digital;
- Hand-written documents and pre-printed forms completed in manuscript;
- E-mail messages, spreadsheets and data from business systems.

- Recorded information, regardless of media or format, created or received in

the course of individual or organisational activity, which provides reliable evidence of policy, actions or decisions.

The School's records should be accurate, up to date and the authoritative version should be available to facilitate the provision of an excellent service and be available for access to information requests. Records require proper management throughout their life from creation to disposal. The guidelines produced by the Records Management Society and National Archives should be used as an aid to assist with best practice:
http://www.nationalarchives.gov.uk/information-management/legislation/data-protection.htm
http://www.irms.org.uk/

Who is covered by this policy

This policy applies to all employees of the School (permanent and temporary, agency), contractors and consultants who have access to records. The same principles should also apply to collaborative working with partners.

This policy and the framework of supporting policies, standards and guidance, aims to make all staff and third parties aware of their responsibilities and what they must do to properly manage the Schools records and information.

This policy requires contracts and agreements to contain appropriate requirements for records and information to be managed in line with this policy and supporting standards and guidance where:

- Contractors or other bodies create or receive and hold records on behalf of the School
- Records are created or received and held as part of collaborative working.

Where there is a need to share records and information a formal data sharing protocol or similar agreement should be agreed prior to information being shared. More details about sharing can be found in the *School's Sharing Policy.*

Record creation and record keeping

There are 4 stages to Records Management:

1. Create or receive information in the form of records
2. Classify records in a logical system by use of a file plan
3. Maintain and use the records
4. Destroy or archive the records in line with our retention guidelines

All records must be authentic and reliable. An authentic record is one that can be proven:
- to be what it purports to be
- to have been created or sent by the person purported to have created or sent it, and
- to have been created or sent at the time purported

A reliable record is one whose contents can be trusted as a full and true and accurate representation of the transactions, activities or facts and can be depended upon in the course of subsequent transactions or activities.

The School must have in place a record keeping system which documents its activities and allows for quick and easy retrieval of information. This must include:

- A logical naming convention to enable accurate filing and retrieval of records
- Allocation of appropriate metadata for electronic records to facilitate accurate retrieval
- Consistent version control procedures
- Consistent and appropriate security classification of records Clearly documented authorship and ownership of records

2. Collection of data

The General Data Protection Regulation requires all data controllers to process personal and sensitive data fairly and lawfully.

When collecting personal and/or sensitive data from individuals it is important that they understand who we are and what their data is being collected for. Rushey Green Primary School ensures that this is followed by providing parents/guardians with the School's Privacy Notice (also called Fair Processing Notice) when a child first starts at the school, as well as to staff, at the beginning of their employment with the school. Rushey Green Primary School also uses privacy / fair processing notices when collecting any further data on forms (paper or electronic).

The school's Privacy Notice states our legal basis for processing data, our data retention periods and of the indivuduals' right to complain to the Information Commissioner's Office (ICO) if they think there is a problem with the way we are dling their data. Our privacy notice will always state who the data controller is (the school), the purpose or purposes for which the information (that we are now collecting) will be processed; and any further information which is necessary in the specific circumstances to enable the processing to be fair.

Please see the School's Privacy Notice for more details.

Some personal and/or sensitive data will be collected throughout a pupil or member of staff's time at the school. This data will be kept securely protected at all times and could be subject to any 'Access to Information' requests. Data should only be retained in line with retention periods and holding it indefinatley could result in a data breach. *Please see School's Retention & Destruction of Records schedule.*

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

When collecting data, the school will need to explain the legal basis for processing this data, the school's retention periods and the right individuals have to complaint to the Information Commissioner's Office (ICO) if they think there is a problem with the way the school is handling their data. The school will need a parent/guardian's consent in order to offer online services to children under 13 lawfully. This consent has to be verifiable and the school's Privacy Notice must be written in concise and clear language to ensure it is easy to understand by children.

3.

4. Accuracy of data

Is it important to ensure that we have an accurate record of any personal data that we hold on children, parents, guardians/carers and members of staff. This data must also be kept up to date where necessary (i.e. next of kin details, contact details, diatery needs, SEN) and where, if this data becomes innacurate or out of date, a child/individual could be put at risk. Inaccurate data could also put the school in breach of the General Data Protection Regulation 2016.

To comply with these provisions we will:

- take steps to ensure the accuracy of any personal data we obtain;
- ensure that the source of any personal data is clear and concise;
- carefully consider any challenges to the accuracy of information;
- consider whether it is necessary to update the information, and
- carry out reviews to confirm data held isaccurate and up to date.

The below information will be updated on an annual basis by issuing enquiry letters.

5. Security of electronic and paper records/documents inside of school premises

The loss of electronic or paper personal/sensitive data, could lead to a serious breach. A serious data breach may require Rushey Green Primary School to notify the Information Commissioner's Office and this could lead to a monetary penalty being levied.

Electronic records should be kept securely, ensuring appropriate and up-to-date encryption software, as well as individual logging passwords and PINs are in place when accessing these records. Safety measures such as routinely back ups of data and software to facilitate audit trails should also be set. Servers should be kept in secure rooms and doors to these rooms should be locked when not in use.

Physical records/paper documents containing personal/sensitive data, should be kept in locked cabinets and, where possible, these cabinets should be fire proof and kept elevated off the ground to prevent damage in case of flooding. An appropriate logging system should also be in place to ensure audit trails can be completed to check who have had access to what record.

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

Paper records which contains personal/personal sensitive data must only be taken off school premises if that data is not accessible via an encrypted device. When paper documents are taken off site, they must be approved and kept to a minimum. Paper documents which contain personal/personal sensitive data must be transported from one location to another in

a lockable bag provided at the school office, carried across the body where possible and kept locked at all times. Under no circumstances should papers be removed from the bag during transit and the bags should never be left unattended at any time (i.e. left in cars overnight, put on the seat next to you on public transport). A register must also be maintained to evidence any data removed from the School with senior management approval. When the data is returned back to the school it must be signed back in. This creates a concise audit trail to ensure that all data is returned and accounted for.

School should avoid taking original documents off premises at all times in case of loss or theft. If documents need to be taken out of the school premises, it is good practice to keep a copy of the data taken. This will provide the school with a record in case this data is lost in transit – the school will still have a record of the data missing and will know the severity of the data compromised. Once the data is back at school site, the copy must be appropriately destroyed (i.e. shred it with a cross cut shredder)

7. Sending information by post

The use of post should be avoided where possible due to the risks. The loss of paper records which contain personal/sensitive data could lead to a serious breach. A serious data breach may require Rushey Green Primary School to notify the Information Commissioner's Office and this could lead to a monetary penalty being levied.

Do not use standard postal services when sending personal, personal sensitive or confidential information as there would be significant impact on its loss. You should look at reducing the risk by using alternative delivery methods:

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

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

Hand Delivery of Files and other items

Pupil Files and any other hand delivered schools data must be handled securely and with care while off schools premises.

Members of staff that are asked to hand deliver schools data on behalf of the school must

comply with the following:

- Transported securely in a lockable bag
- Check items/package is clearly marked with the address destination
- Check the items/packages are sealed before they leave school premises
- Check items are being delivered to the correct destination
- Use a prefilled sheet which records all items being delivered & gain a signature from an individual at the delivery address
- Staff will need to go straight home on the days approval has been granted to remove case files, papers and any other documents from the office

Staff must not:

- Leave items with un-identified individuals
- Deliver and not gain a signature
- Take items home to deliver the next day
- Leave bags containing school information unattended at any time (i.e. left in cars overnight, put on the seat next to you on public transport)
- Ask someone else to deliver items without authorisation from the SLT

8. 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

9. Clear Desk and Screen

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

- Clear out desk draws and cupboards on a planned basis

- Use the cross cut shredder provided in your school to dispose of confidential office paper when it is on longer needed

- Where possible, do not print off confidential e-mail to read as this will generate extra paper and extra risk

- If you print confidential information collect it from the printer immediately

- Dispose (shred or lock away) any personal / personal sensitive / confidential data left on photocopiers / printers if found unnatended in the office.

- When sending a fax ensure you send it to the correct fax number, notify the recipient and confirm it has been received.

- 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 compueter/laptop monitor. Make sure systems/documents 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 must be checked and cleared out daily to avoid confidential data being comprised.

- Do not use confidential paper as scrapt and do not put confidential paper in recycling bins – always put confidential paper in the confidential waste

10. Schools Retention Schedule / Secure Disposal of Records & ICT equipment

Rushey Green Primary School has a current and up to date retention schedule which sets out how long personal and/or personal sensitive data must be held for in line with the General Data Protection Regulation. Keeping records longer than necessary could result in a data breach. Data Protection Principle 5 states 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

Personal and/or personal sensitive data must be destroyed in line with the schools retention schedule which can be requested from the schools head teacher. It is of the upmost 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. This will also help if in future a former pupil or former member of staff request to see their data as part of a subject access request, the school must have a record of whether or not their files have been retained or destroyed.

See Appendix 2 – Destruction of Records Spreadsheet template/guide

If Rushey Green Primary School has any unwanted ICT equipment that is no longer in use and needs to be securely disposed of, you can contact the schools data protection officer who will provide you with the appropriate contact details for the school to arrange secure disposal through the Council's ICEX contract.

Please see the School's Destruction of Records Booklet for more details.

11. Sharing data with third parties / DPIAs and ISAs

When there is a requirement for Rushey Green Primary School to share personal and/or personal sensitive data with third party providers, it is mandatory to adopt a privacy by design approach and to carry out a Data Protection Impact Assessment (DPIA) as part of this.

DPIAs are used to identify and reduce the privacy risks of any change in the way data is processed. A DPIA will help ensure that any changes will comply with data protection and guarantee the same level of security/privacy in regards of personal, sensitive information. It can also help design more efficient and effective processes for handling personal, sensitive data. (Please refer to the DPIA template)

When sharing personal and/or personal sensitive data there must be sufficient data sharing protocols in place. After a DPIA has been completed, the way we share information can be recorded in a contract, within a confidentiality statement or, in an Information Sharing Agreement (ISA).

ISAs (sometimes known as Data Sharing Protocols) set out a common set of rules to be adopted by the various organisations involved in an information sharing operation.

The main organisations our school share personal information with are:

- Local authorities including children social care, Attendance and Welfare, Early Intervention Service
- Government departments/ DFE
- Other schools and educational bodies
- The police service
- Health services including School Nursing Service, GPs, and CAMHS (children and mental health service).
- Software providers

The General Data Protection Regulation 2016 and Human Rights law are not barriers to justify information sharing. Where the school has concerns about the safety of a child, sometimes information will be shared with Children's Social Care through the recognised channels, always ensuring personal information is shared appropriately and securely. Where possible, information should be shared with informed consent, however, they might be cases where information may be shared without consent, such as where the safety or well-being of the child may be at risk.

Necessary, proportionate, relevant, adequate, accurate, timely and secure: always ensure that the information the school shares is necessary for the purpose for which you are sharing it for, is shared only with those individuals who need to have it, is accurate and up-to-date, is

shared in a timely fashion and is shared securely. Always keep a record of the school's decision and the reasons for it – whether it is to share information or not. If the school decides to share, then record what it was shared, with whom and for what purpose. In these circumstances, when deciding whether to share information or not, the most important consideration the school should make is whether sharing information is likely to safeguard and protect a child.

Please see School's Sharing Policy for more details.

12. Responsibilities

All information collected, and records created by Rushey Green Primary 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.

The school's Data Protection Officer is responsible for;

- Ensuring that this policy is being followed

- Ensuring that the management of schools records is kept up to date with regular checks
- Advising school staff on records management, policy and procedures
- Implementing the Records Management policy
- Maintaining the schools retention schedules
- Ensuring the destruction of records process is followed
- And ensuring all data is retained securely

All Staff have a responsibility to abide by this records management policy.

The Headteacher will meet with the schools data protection officer on a regular basis where records management tasks, ideas & issues will be discussed.

The data protection adviser is available to provide advice and guidance to the school as and when required from 9am-5pm Monday to Friday, by phone on **020 8314 8183** or **07825762328** or e-mail Schoolsdpa@lewisham.gov.uk

13. What happens if this policy is breached

All Staff have a responsibility to abide by the records management policy. Any breach of this policy could lead to disciplinary action being taken. Please see breach policy for more details.

14. Review

This policy will be reviewed as and when required.

APPENDIX 1-

Privacy / Fair Processing Notice on forms

'Why and how we collect and use your data'

<u>The General Data Protection Regulation 2016</u>

For the purposes of the General Data Protection Regulation 2016, Rushey Green Primary School is the data controller and therefore is responsible for the information it collects.

The information in this form is being collected for ……...
.....……
…
……..……
… ……..

The information on this form will also be shared with *(third parties and why it will be shared to be added)* 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 Rushey Green Primary School handles your data please see the schools privacy notice which is available at the school office.

APPENDIX 2-

Destruction of Records Spreadsheet template/guide

