# Rosehill Infant and Nursery School

# Retention Policy and Data Protection Breach & Non Compliance Procedure

**Policy Approval – 15th June 2023**

**Review – June 2025**

**Approved:**

**……..Headteacher Date: ……**

**……...Chair of Governors Date: ……..**

## Contents:

## Statement of intent

**Rosehill Infant and Nursery School** is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the GDPR, the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the UK GDPR and Data Protection Act 2018.

# 1. Legal framework

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

- **General Data Protection Regulation GDPR**
- **Freedom of Information Act 2000**
- **Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)**
- **Data Protection Act 2018**

1.2. This policy also has due regard to the following guidance:

- **Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools'**
- **DfE (2023) 'Data protection: a toolkit for schools'**

1.3. This policy will be implemented in accordance with the following school policies and procedures:

- **Data Protection Policy**
- **Freedom of Information Policy**
- **Disposal of Records Log**
- **Information Asset Register**

# 2. Responsibilities

2.1. The school as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The headteacher holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The data protection officer (DPO) is responsible for the management of records at Rosehill Infant and Nursery School.

2.4. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an three year basis, in conjunction with the head teacher/school business manager..

2.5. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of safely and correctly.

2.6. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy

## 3. Management of pupil records

3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievement.

3.2. The following information is stored within a pupil record, and will be easily accessible:

- **Forename, surname, gender and date of birth**
- **Unique pupil number**
- **Note of the date when the file was opened**
- **Note of the date when the file was closed, if appropriate**
- **Ethnic origin, religion and first language (if not English)**
- **Any preferred names**
- **Position in their family, e.g. eldest sibling**
- **Emergency contact details and the name of the pupil's doctor**
- **Any allergies or other medical conditions that are important to be aware of**
- **Names of parents, including their home address(es), national insurance number and telephone number(s)**
- **Name of the school, admission number, the date of admission and the date of leaving, where appropriate**
- **Any other agency involvement, e.g. speech and language therapist**

3.3. The following information is stored in a pupil record, and will be easily accessible:

- **Admissions form**
- **Details of any SEND**
- **If the pupil has attended an early years setting, the record of transfer**
- **Annual written reports to parents**
- **National curriculum and agreed syllabus record sheets**
- **Notes relating to major incidents and accidents involving the pupil**

- **Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan**
- **Medical information relevant to the pupil's on-going education and behaviour**
- **Any notes indicating child protection disclosures and reports are held**
- **Any information relating to exclusions**
- **Any correspondence with parents or external agencies relating to major issues, e.g. mental health**
- **Notes indicating that records of complaints made by parents or the pupil are held**

The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the school office:

- **Attendance registers and information**
- **Absence notes and correspondence**
- **Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.**
- **Consent to administer medication and administration records**
- **Copies of pupil birth certificates, passports etc.**
- **Correspondence with parents about minor issues, e.g. behaviour**
- **Pupil work**
- **Previous data collection forms that have been superseded**

3.4. Electronic copies of disclosures and reports relating to child protection are stored on a secure MIS (C-POMs) restricted access. Hard copies are kept in a locked cabinet with restricted access in a sealed envelope. When the record is transferred to a feeder school the information will be hand delivered in a sealed envelope marked private and confidential and a signature of the recipient will be obtained and kept on file.

3.5. Hard copies of complaints made by parents or pupils are stored in a file in the headteacher's office – a note indicating this is marked on the pupil's file.

3.6. Actual copies of accident and incident information are stored separately in a locked cupboard in the Health & Safety file in the SLT office. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.7. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend.

3.8. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the administrator responsible for disposing records, will remove these records.

3.9. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 12 of this policy outlines how electronic records will be transferred.

3.10. The school will not keep any copies of information stored within a pupil's record, unless there is ongoing legal action at the time during which the pupil leaves the school. The responsibility for these records will then transfer to the next school that the pupil attends.

3.11. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

## 4. Retention of pupil records and other pupil-related information

4.1. The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.

4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

| Type of file | Retention period | Action taken after retention period ends |
|---|---|---|
| **Personal identifiers, contacts and personal characteristics** | | |
| Images used for identification purposes | For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month | Securely disposed of |
| Images used in displays in schools | Whilst the pupil is at school | Securely disposed of |
| Images used for marketing purposes, or other | In line with the consent period | Securely disposed of |
| Biometric data | For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month | Securely disposed of |

| | | |
|---|---|---|
| Postcodes, names and characteristics | Whilst the pupil is at school, plus five years | Securely disposed of |
| House number and road | For the duration of the event/activity, plus one month | Securely disposed of |
| **Admissions** | | |
| Register of admissions | Every entry in the admissions register will be preserved for a period of three years after the date on which the entry was made | Information is reviewed and the register may be kept permanently |
| Admissions (where the admission is successful) | Date of admission, plus one year | Securely disposed of |
| Admissions appeals (where the appeal is unsuccessful) | Resolution of the case, plus one year | Securely disposed of |
| Proof of address (supplied as part of the admissions process) | Whilst the pupil remains at the school | Securely disposed of |
| Supplementary information submitted, including religious and medical information etc. (where the admission was successful) | Information added to the pupil file | Securely disposed of |
| Supplementary information submitted, including religious and medical information etc. (where the admission was not successful) | Retained until the appeals process is complete | Securely disposed of |
| All records relating to the creation and implementation of the Admissions Policy | Life of the policy, plus three years and then review | Securely disposed of |
| **Pupils' educational records** | | |
| Pupils' educational records | Whilst the pupil remains at the school | Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the LA and retained for the statutory period |
| Public examination results | Added to the pupil's record and transferred to next school | Returned to the examination board |

| | | |
|---|---|---|
| | Copies with pupils' names are held whilst the pupil is at school, plus five years<br><br>Copies with pupils' names removed are held for 25 years after the pupil's date of birth | |
| Internal examination results | Added to the pupil's record and transferred to next school<br><br>Copies with the pupil's personal data are held whilst the pupil is at school, plus five years<br><br>Copies with personal data removed are held for 25 years after the pupil's date of birth | Securely disposed of |
| Behaviour records | Added to the pupil's record and transferred to the next school<br><br>Copies are held whilst the pupil is at school, plus one year | Securely disposed of |
| Exclusion records | Added to the pupil's record and transferred to the next school<br><br>Copies are held whilst the pupil is at school, plus one year | Securely disposed of |
| Child protection information held on a pupil's record | Stored in a sealed envelope for the same length of time as the pupil's record<br><br>Records also subject to any instruction given by the Independent Inquiry into Child Sex Abuse (IICSA) | Securely disposed of – shredded |

| | | |
|---|---|---|
| | | |
| Child protection records held in a separate file | 25 years after the pupil's date of birth<br><br>Records also subject to any instruction given by the IICSA | Securely disposed of – shredded |
| Timetable | Current academic year, plus one year | Review at the end of each year and allocate a further retention period or securely dispose of |
| Schemes of work | Current academic year, plus one year | Review at the end of each year and allocate a further retention period or securely dispose of |
| Curriculum returns | Current academic year, plus three years | Securely disposed of |
| Class record books | Current academic year, plus one year | Review at the end of each year and allocate a further retention period or securely dispose of |
| Mark books | Current academic year, plus one year | Review at the end of each year and allocate a further retention period or securely dispose of |
| Record of homework set | Current academic year, plus one year | Review at the end of each year and allocate a further retention period or securely dispose of |
| Pupils' work | Current academic year, plus one year | Review at the end of each year and allocate a further retention period or securely dispose of |
| Education, training or employment destinations data | Whilst the pupil is at the school, plus three years or from the end of KS4, whichever is earliest | Securely disposed of |
| **Attendance** | | |
| Attendance registers | Every entry is retained for a period of three years after the date on which the entry was made | Securely disposed of |
| Correspondence relating to any absence (authorised or unauthorised) | Current academic year, plus two years | Securely disposed of |

| | | |
|---|---|---|
| **Medical information and administration** | | |
| Permission slips | For the duration of the period that medication is given, plus one month | Securely disposed of |
| Medical conditions – ongoing management | Added to the pupil's record and transferred to the next school<br><br>Copies held whilst the pupil is at school, plus one year | Securely disposed of |
| Medical incidents that have a behavioural or safeguarding influence | Added to the pupil's record and transferred to the next school<br><br>Copies held whilst the pupil is at school, plus 25 years | Securely disposed of |
| **SEND** | | |
| SEND files, reviews and EHC plans, including advice and information provided to parents regarding educational needs and accessibility strategy | The pupil's date of birth, plus 31 years | Securely disposed of |
| **Curriculum management** | | |
| SATs results | Moves with the child to their feeder school or 25 years after the pupil's date of birth (as stated on the pupil's record) | Securely disposed of |
| Examination papers | Until the appeals/validation process has been completed | Securely disposed of |
| Published Admission Number (PAN) reports | Current academic year, plus six years | Securely disposed of |
| Valued added and contextual data | Current academic year, plus six years | Securely disposed of |
| Self-evaluation forms | Current academic year, plus six years | Securely disposed of |

| | | |
|---|---|---|
| Pupils' work | Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year | Securely disposed of |
| **Extra-curricular activities** | | |
| Field file – information taken on school trips | Until the conclusion of the trip, plus one month<br><br>Where a minor incident occurs, field files are added to the core system as appropriate | Securely disposed of |
| Financial information relating to school trips | Whilst the pupil remains at school, plus one year | Securely disposed of |
| Parental consent forms for school trips where no major incident occurred | Until the conclusion of the trip | Securely disposed of |
| Parental consent forms for school trips where a major incident occurred | 25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils) | Securely disposed of |
| Educational visitors in school – sharing of personal information | Until the conclusion of the visit, plus one month | Securely disposed of |
| **Family liaison officers and home-school liaison assistants** | | |
| Day books | Current academic year, plus two years | Reviewed and destroyed if no longer required |
| Reports for outside agencies | Duration of the pupil's time at school | Securely disposed of |
| Referral forms | Whilst the referral is current | Securely disposed of |
| Contact data sheets | Current academic year | Reviewed and destroyed if no longer active |
| Contact database entries | Current academic year | Reviewed and destroyed if no longer required |
| Group registers | Current academic year, plus two years | Securely disposed of |

| Catering and free school meal management | | |
|---|---|---|
| Meal administration | Whilst the pupil is at school, plus one year | Securely disposed of |
| Meal eligibility | Whilst the pupil is at school, plus five years | Securely disposed of |

## 5. Retention of staff records

5.1. The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

| Type of file | Retention period | Action taken after retention period ends |
|---|---|---|
| **Operational** | | |
| Staff members' personal file | Termination of employment, plus six years, unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file will be retained until the IICSA enquiries are complete | Securely disposed of |
| Annual appraisal and assessment records | Current academic year, plus six years | Securely disposed of |
| Sickness absence monitoring (where sickness pay is not paid) | Current academic year, plus three years | Securely disposed of |
| Sickness absence monitoring (where sickness pay is paid) | Current academic year, plus six years | Securely disposed of |
| Staff training (where training leads to CPD) | Length of time required by the CPD professional body | Securely disposed of |
| Staff training (where the training relates to pupils, e.g. safeguarding or other pupil-related training) | Date of the training, plus 40 years | Securely disposed of |
| Staff training (except where the training relates to dealing with pupils, e.g. first aid or health and safety) | Retained in the personnel file | Securely disposed of |
| **Recruitment** | | |

| | | |
|---|---|---|
| Records relating to the appointment of a new headteacher (unsuccessful attempts) | Date of appointment, plus six months | Securely disposed of |
| Records relating to the appointment of a new headteacher (successful attempts) | Added to personnel file and retained until the end of appointment, plus six years, except in cases of negligence or claims of child abuse, then records are retained for at least 15 years | Securely disposed of |
| Records relating to the appointment of new members of staff or governors (unsuccessful candidates) | Date of appointment of successful candidate, plus six months | Securely disposed of |
| Pre-employment vetting information (successful candidates) | For the duration of the employee's employment, plus six years | Securely disposed of |
| DBS certificates | Up to six months | Securely disposed of |
| Proof of identify as part of the enhanced DBS check | If it is necessary to keep a copy, it will be placed in the staff member's personnel file | Securely disposed of |
| Evidence of right to work in the UK | Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years | Securely disposed of |
| **Disciplinary and grievance procedures** | | |
| Child protection allegations, including where the allegation is unproven | Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer<br><br>If allegations are malicious, they are removed from personal files<br><br>If allegations are found, they are kept on the personnel file and a copy is provided to the person concerned | Reviewed and securely disposed of – shredded |

| | | |
|---|---|---|
| | unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file is retained until IICSA enquiries are complete | |
| Oral warnings | Date of warning, plus six months | Securely disposed of – if placed on staff personal file, removed from file |
| Written warning – level 1 | Date of warning, plus six months | Securely disposed of – if placed on staff personal file, removed from file |
| Written warning – level 2 | Date of warning, plus 12 months | Securely disposed of – if placed on staff personal file, removed from file |
| Final warning | Date of warning, plus 18 months | Securely disposed of – if placed on staff personal file, removed from file |
| Records relating to unproven incidents | Conclusion of the case, unless the incident is child protection related and is disposed of as above | Securely disposed of |

## 6. Retention of senior leadership and management records

6.1. The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

6.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

| Type of file | Retention period | Action taken after retention period ends |
|---|---|---|
| **Governing board** | | |
| Agendas for governing board meetings | One copy alongside the original set of minutes – all others disposed of without retention | Securely disposed of |

| | | |
|---|---|---|
| Original, signed copies of the minutes of governing board meetings | Permanent – all other copies disposed of without retention | Shredded if they contain any sensitive or personal information, but the local archives will be consulted first |
| Reports presented to the governing board that are referred to in the minutes | Permanent – all others disposed of without retention | Local archives consulted and then securely disposed of |
| Meeting papers relating to the annual parents' meeting | Date of meeting, plus a minimum of six years | Securely disposed of |
| Instruments of government, including articles of association | Permanent | Local archives consulted and then securely disposed of |
| Trusts and endowments managed by the governing board | Permanent | Local archives consulted and then securely disposed of |
| Action plans created and administered by the governing board | Until superseded or whilst relevant | Securely disposed of |
| Policy documents created and administered by the governing board | Until superseded or whilst relevant | Securely disposed of |
| Records relating to complaints dealt with by the governing board or headteacher | Current academic year, plus six years<br><br>If negligence is involved, records are retained for the current academic year, plus 15 years<br><br>If child protection or safeguarding issues are involved, the records are retained for the current academic year, plus 40 years | Reviewed for further retention in case of contentious disputes, then securely disposed of |
| Annual reports required by the DfE | Date of report, plus 10 years | Securely disposed of |
| Proposals concerning changing the status of the school | Date proposal accepted or declined, plus three years | Securely disposed of |

| | | |
|---|---|---|
| Records relating to the appointment of co-opted governors | Date of election, plus six months | Securely disposed of |
| Records relating to the election of the chair of the governing board and the vice chair | Destroyed after the decision has been recorded in the minutes | Securely disposed of |
| Scheme of delegation and terms of reference for committees | Until superseded or whilst relevant | Reviewed and offered to the local archives if appropriate |
| Meeting schedule | Current academic year | Standard disposal |
| Register of attendance at full governing board meetings | Date of last meeting in the book, plus six years | Securely disposed of |
| Records relating to governor monitoring visits | Date of the visit, plus three years | Securely disposed of |
| **[Academies or maintained schools converting to academy status only]** All records relating to the conversion of the school to academy status | Permanent | Local archives are consulted before disposal |
| Correspondence sent and received by the governing board or headteacher | Current academic year, plus three years | Securely disposed of |
| Records relating to the appointment of the clerk to the governing board | Date on which the clerk's appointment ends, plus six years | Securely disposed of |
| Records relating to the terms of office of serving governors, including evidence of appointment | Date on which the governor's appointment ends, plus six years | Securely disposed of |
| Records relating to governor declaration against disqualification criteria | Date on which the governor's appointment ends, plus six years | Securely disposed of |
| Register of business interests | Date the governor's appointment ends, plus six years | Securely disposed of |
| Governor code of conduct | Dynamic document – kept permanently | Securely disposed of |

| | | |
|---|---|---|
| Records relating to the training required and received by governors | Date the governor steps down, plus six years | Securely disposed of |
| Records relating to the induction programme for new governors | Date on which the governor's appointment ends, plus six years | Securely disposed of |
| Records relating to DBS checks carried out on the clerk and members of the governing board | Date of the DBS check, plus six months | Securely disposed of |
| Governor personnel files | Date on which the governor's appointment ends, plus six years | Securely disposed of |
| **Headteacher and SLT** | | |
| Log books of activity in the school maintained by the headteacher | Date of last entry, plus a minimum of six years | Reviewed and offered to the local archives if appropriate |
| Minutes of SLT meetings and the meetings of other internal administrative bodies | Date of the meeting, plus three years | Reviewed annually and securely disposed of if not needed |
| Reports created by the headteacher or SLT | Date of the report, plus a minimum of three years | Reviewed annually and securely disposed of if not needed |
| Records created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities | Current academic year, plus six years | Reviewed annually and securely disposed of if not needed |
| Correspondence created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities | Date of correspondence, plus three years | Securely disposed of |
| Professional development plan | Held on the individual's personnel record. If not, then it is retained for the duration of the plan, plus six years | Securely disposed of |
| SDP | Duration of the plan, plus three years | Securely disposed of |

## 7. Retention of health and safety records

7.1. The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

| Type of file | Retention period | Action taken after retention period ends |
|---|---|---|
| **Health and safety** | | |
| Health and safety policy statements | Duration of policy | Securely disposed of |
| Health and safety risk assessments | Duration of risk assessment, plus three years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred | Securely disposed of |
| Records relating to any reportable death, injury, disease or dangerous occurrence under RIDDOR | Date of incident, plus three years provided that all records relating to the incident are held on the personnel file | Securely disposed of |
| Accident reporting – adults | Three years after the last entry in the accident reporting book | Securely disposed of |
| Accident reporting – pupils | Three years after the last entry in the accident reporting book | Securely disposed of |
| Control of substances hazardous to health | Current academic year, plus 40 years | Securely disposed of |
| Information relating to areas where employees and persons are likely to come into contact with asbestos | Date of last action, plus 40 years | Securely disposed of |
| Information relating to areas where employees and persons are likely to come into contact with asbestos | Date of last action, plus 40 years | Securely disposed of |
| Fire precautions log books | Current academic year, plus three years | Securely disposed of |
| Visitors book | End of year plus 6 years | Securely disposed of |
| Declaration for visitors – used for covid-19 track and trace | 4 weeks from last day of the week (Friday) | Securely disposed of |
| Health and safety file to show current state of buildings, including all alterations (wiring, | Permanent | Passed to new owner on sale or transfer of building |

| | | |
|---|---|---|
| plumbing, building works etc.) to be passed on in the case of change of ownership | | |

## 8. Retention of financial records

8.1. The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

| Type of file | Retention period | Action taken after retention period ends |
|---|---|---|
| **Payroll pensions** | | |
| Maternity pay records | Current academic year, plus three years | Securely disposed of |
| Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Current academic year, plus six years | Securely disposed of |
| Personal bank details | Until superseded, plus three years | Securely disposed of |
| Timesheets | Current academic year, plus three years | Securely disposed of |
| **Risk management and insurance** | | |
| Employer's liability insurance certificate | Closure of the school, plus 40 years | Securely disposed of |
| **Asset management** | | |
| Inventories of furniture and equipment | Current academic year, plus six years | Securely disposed of |
| Burglary, theft and vandalism report forms | Current academic year, plus six years | Securely disposed of |
| | | |

| | | |
|---|---|---|
| Annual accounts | Current academic year, plus six years | Disposed of against common standards |
| Loans and grants managed by the school | Date of last payment, plus 12 years | Information is reviewed then securely disposed of |
| All records relating to the creation and management of budgets | Duration of the budget, plus three years | Securely disposed of |
| Invoices, receipts, order books, requisitions and delivery notices | Current financial year, plus six years | Securely disposed of |
| Records relating to the collection and banking of monies | Current financial year, plus six years | Securely disposed of |
| Records relating to the identification and collection of debt | Final payment, plus six years | Securely disposed of |
| **Contract management** | | |
| All records relating to the management of contracts under seal | Last payment on the contract, plus 12 years | Securely disposed of |
| All records relating to the management of contracts under signature | Last payment on the contract, plus six years | Securely disposed of |
| All records relating to the monitoring of contracts | Life of the contract, plus six or 12 years | Securely disposed of |
| **School fund** | | |
| Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books | Current academic year, plus six years | Securely disposed of |
| **School meals** | | |
| Free school meals registers | Current academic year, plus six years | Securely disposed of |
| School meals registers | Current academic year, plus three years | Securely disposed of |
| School meals summary sheets | Current academic year, plus three years | Securely disposed of |

## 9. Retention of other school records

9.1. The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

| Type of file | Retention period | Action taken after retention period ends |
|---|---|---|
| **Property management** | | |
| Title deeds of properties belonging to the school | Permanent | Held by the LA<br>Transferred to new owners if the building is leased or sold |
| Plans of property belonging to the school | For as long as the building belongs to the school | Held by the LA and school.<br>Transferred to new owners if the building is leased or sold |
| Leases of property leased by or to the school | Expiry of lease, plus six years | Securely disposed of |
| Records relating to the letting of school premises | Current financial year, plus six years | Securely disposed of |
| **Maintenance** | | |
| All records relating to the maintenance of the school carried out by contractors | For as long as the school owns the building and then passed onto any new owners if the building is leased or sold | Securely disposed of |
| All records relating to the maintenance of the school carried out by school employees | For as long as the school owns the building and then passed onto any new owners if the building is leased or sold | Securely disposed of |
| **Operational administration** | | |
| General file series | Current academic year, plus five years | Reviewed and securely disposed of |
| Records relating to the creation and distribution of circulars to staff, parents or pupils | Current academic year, plus one year | Disposed of against common standards |
| Newsletters and other items with short operational use | Current academic year, plus one year | One copy archived, other copies standard disposal |
| Visitors' books and signing-in sheets | Last entry in the logbook, plus six years | Reviewed then securely disposed of |
| Records relating to the creation and management of parent-teacher associations and/or old pupil associations | Current academic year, plus six years | Reviewed then securely disposed of |

| | | |
|---|---|---|
| Walking bus registers | Date of register, plus six years | Securely disposed of |
| School privacy notice which is sent to parents | Until superseded, plus six years | Standard disposal |
| Consents relating to school activities | While pupil attends the school | Secure disposal |

## 10. Retention of emails

10.1. Any user of Group email addresses will have responsibility for managing the account and ensuring the correct disposal of all sent and received emails.

10.2. All staff members with an email account will be responsible for managing their inbox.

10.3. Emails can act as evidence of the school's activities, i.e. in business and fulfilling statutory duties, so all relevant emails (e.g. invoices) will be retained for at least 12 months. The owner of these e-mails is responsible for correct deletion.

10.4. Invoices received and sent in emails will be printed off and retained in accordance with section 8 of this policy.

10.5. All users are to delete their e-mails after 12 months, unless stated otherwise.

10.6. Correspondence created by the SLT and other members of staff with administrative responsibilities will be retained for three years before being reviewed and, if necessary, securely disposed of.

10.7. Personal emails, i.e. emails that do not relate to work matters or are from family members, will be deleted as soon as they are no longer needed.

10.8. Staff members will review and delete any emails they no longer require at the end of every term.

10.9. Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives.

10.10. Staff members will be aware that the emails they send could be required to fulfil a SAR or freedom of information (FOI) request. Emails will be drafted carefully, and staff members will review the content before sending.

10.11. Individuals, including children, have the right to submit an SAR to gain access to their personal data to verify the lawfulness of the processing – this includes accessing emails.

10.12. All SARs will be handled in accordance with the school's Data Protection Policy.

10.13. FOI requests will be handled in accordance with the school's Freedom of Information Policy.

10.14. When handling a request for information, the DPO will speak to the requestor to clarify the scope of the request and whether emails will be required to fulfil the SAR or FOI request.

10.15. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.16. All requests will be responded to without delay and at the latest, within one month of receipt.

10.17. If a request is manifestly unfounded, excessive or repetitive, a fee will be charged. All fees will be based on the administrative cost of providing the information.

10.18. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.19. Staff members will discuss any queries regarding email retention with the DPO.

## 11. Identifying information

11.1. Under the GDPR, all individuals have the right to data minimisation and data protection by design and default – as the data controller, the school ensures appropriate measures are in place in order for individuals to exercise this right.

11.2. Wherever possible, the school uses pseudonymisation, also known as the 'blurring technique', to reduce risk of identification.

11.3. Once an individual has left the school, if identifiers such as names and dates of birth are no longer required, these are removed or less specific personal data is used, e.g. the month of birth rather than specific date – the data is blurred slightly.

11.4. Where data is required to be retained over time, e.g. attendance data, the school removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

## 12. Storing and protecting information

12.1. The DPO will undertake a business impact assessment to identify which records are vital to school management and these records will be stored in the most secure manner.

12.2. The ICT Company, Mercury will conduct a back-up of information on a daily basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

12.3. Where possible, backed-up information will be stored off the school premises, using a central back-up service. The DPO will ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored on it.

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

12.5. Any room or area where personal or sensitive data is stored will be locked when unattended.

12.6. Confidential paper records are not left unattended or in clear view when held in a location with general access.

12.7. 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.

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

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

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

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

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

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

12.14. Emails containing sensitive or confidential information are password-protected or sent via a secure encrypted or data transfer system to ensure that only the

recipient is able to access the information. The password will be shared with the recipient in a separate email.

12.15. Personal information is never put in the subject line of an email.

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

12.17. Information will not be sent by fax.

12.18. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an 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.

12.19. If documents that have been taken off the school premises will be left unattended, the staff member will leave the documents in the locked boot of a car or keep them on their person.

12.20. Before sharing data, staff always ensure that:

- **They have consent from data subjects to share it.**
- **Adequate security is in place to protect it.**
- **The data recipient has been outlined in a privacy notice.**

12.21. The school has data sharing agreements with all data processors and third parties with whom data is shared. These agreements are developed by the DPO and cover information about issues such as access controls and permissions.

12.22. The school has data sharing agreements with all data processors and third parties with whom data is shared. These agreements are developed by the DPO and cover information about issues such as access controls and permissions.

12.23. All staff members will implement a ‘clear desk policy’ to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

12.24. 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.

12.25. Staff are required to use their school login details to use photocopiers and printers

12.26. The physical security of the school's buildings and storage systems, and access to them, is reviewed termly by the School Business Manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the headteacher and extra measures to secure data storage will be put in place.

12.27. The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

12.28. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

12.29. Any damage to or theft of data will be managed in accordance with the school's Data Protection Breach & Non Compliance Procedure (appendix 1)

## 13. Accessing information

13.1. Rosehill Infant and Nursery School is transparent with data subjects, the information we hold and how it can be accessed.

13.2. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, 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 provide and withdraw consent to information being held.**
- **Understand what the school is doing to comply with its obligations under the GDPR.**

13.3. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

13.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

13.5. Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

13.6. The school will adhere to the provisions outlined in the school's Data Protection Policy when responding to requests seeking access to personal information.

## 14. Digital continuity

14.1. Digital data that is retained for longer than six years and contains personal data will be named on the schools data mapping .

14.2. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 12 of this policy.

14.3. Memory sticks will never be used to store digital data, subject to a digital continuity statement.

14.4. The IT technician will review new and existing storage methods annually.

## 15. Information audit

15.1. The school conducts information audits against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Knowledge
- Apps/Portals

15.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

15.3. The DPO is responsible for completing the information audit. The information audit will include the following:

- The school's data needs
- The information needed to meet those needs

- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

15.4. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

15.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Information Asset Register.

15.6. The information displayed on the Information Asset Register will be shared with the headteacher to gain their approval.

## 16. Disposal of data

16.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

16.2. Where disposal of information is outlined as secure disposal, this will be shredded or pulped and electronic information will be scrubbed clean and, where possible, cut, archived or digitalised. The persons responsible for deletion of files will keep a record of all files that have been destroyed and share it with the school business manager.

16.3. Where the disposal action is indicated as reviewed before it is disposed, the Head teacher, School business manager will review the information against its administrative value – if the information should be kept for administrative value, the School business manager will keep a record of this.

16.4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

16.5. Where information has been kept for administrative purposes, the School business manager will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

16.6. Where information must be kept permanently, this information is exempt from the normal review procedures

16.7. Records and information that might be of relevant to the Independent Inquiry into Child Sexual Abuse (IICSA) will not be disposed of or destroyed

## 17. School closures and record keeping

**Academy conversion**

17.1. If the school closes and subsequently becomes an academy, all records relating to pupils who are transferring to the academy will be transferred.

17.2. If the school will retain the existing building when it converts to an academy, all records relating to the management of the buildings will be transferred.

17.3. All other records created and managed when the school was part of the LA will become the responsibility of the LA.

**Sale or re-use of the site**

17.4. If the school site is being sold or re-allocated to another use, the LA will take responsibility for the records from the date the school closes.

**Merger of schools**

17.5. If the school merges with another school to create one school, the new school will be responsible for retaining all current records originating from the former schools.

17.6. The DPO will determine the outcome of each group of records; these outcomes are as follows:

- Securely destroy all records that are expired and due for disposal, in accordance with the retention periods outlined in this policy.
- Transfer to the successor school or academy all records that are current and that will be required by the new school or academy.
- Transfer to the LA all records that are dormant but still need to be retained to comply with legal and business retention requirements.
- Transfer to the local record office any records with historical value.

**Managing records**

17.7. The DPO will identify which records need to be destroyed or transferred to the relevant body – they will allocate personnel as necessary to sort through records.

17.8. The DPO will notify the other organisations as soon as possible so that necessary disposal, storage and transfer arrangements can be made. The school's IT provider will also be notified so that arrangements can be made to ensure the safe transfer or deletion of electronic records, including all back-up copies.

17.9. When sorting records, the DPO and their team will:

- Review all records held within the school as soon as notification of closure is received, including paper and electronic records.

- Use the retention periods outlined in this policy to categorise the records into those to be destroyed and those that need to be transferred
- Contact the relevant body to make arrangements for the safe and secure transfer of records.
- Sort, list and box the records in preparation for the transfer, ensuring records are stored in a safe environment whilst awaiting collection.
- Plan how the disposal of records will be undertaken.
- Sort expired records in readiness for confidential disposal, ensuring they are stored securely whilst awaiting disposal.

17.10. All forms of storage will be completely emptied before the building is vacated or before disposal.

17.11. Records awaiting transfer will be held in a secure area.

17.12. The identity of any third parties collecting or disposing of records will be checked and a collection receipt will be obtained.

17.13. Records will be disposed of in line with section 16 of this policy.

17.14. Electronic records will be either transferred to the new body or deleted.

17.15. All IT equipment will be decommissioned

17.16. No records will be left behind once the school building is vacated.

## 18. Monitoring and review

18.1. This policy will be reviewed on an annual basis by the DPO/School business manager in conjunction with the headteacher – the next scheduled review date for this policy is May 2023.

18.2. Any changes made to this policy will be communicated to all members of staff and the governing board.

Appendix 1

# Data Protection Breach & Non Compliance Procedure

All staff, governors and trustees are aware of what to do in the event of a DPA / GDPR breach. The

'Data Breach Flowchart' outlines the process.

The 'Data Breach Form' must be completed and updated as the process progresses.

Most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

## 19. What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Head Teacher, School Business Manager or DPO as soon as possible, this is essential.

The breach notification form will be completed and the breach register updated.
If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.
The breach report will be within 72 hours of becoming aware of the breach.

It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

## 20. Procedure – Breach notification data controller to data subject

For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Head Teacher, School business manager with support from the Data Protection Officer.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

## 21. Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

| Date | Evidence Description | Secure storage location & confirmed date | School Officer |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |