Rosehill Infant and Nursery School

Retention Policy and Data Protection Breach & Non Compliance Procedure

Policy Approval – 12th June 2018

Review – June 2021

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 GDPR, which is effective of 25 May 2018.

1. Legal framework

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

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

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

- **Information Records Management Society (2016) 'Information Management Toolkit for Schools'**
- **DfE (2018) '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**
- **E-security Policy**
- **Disposal of Records Log**
- **Information Asset Register**
- **Archived Files Log**

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 annual 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 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**

- **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**
- **Absence notes**
- **Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.**
- **Correspondence with parents about minor issues, e.g. behaviour**

3.4. Electronic copies of disclosures and reports relating to child protection are stored on a secure section of the schools server with 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 11 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	Whilst the pupil remains at the school, plus one year	Information is reviewed and the register may be kept permanently
Admissions appeals	Whilst the pupil remains at school, plus five years	Securely disposed of
Proof of address (supplied as part of the admissions process)	Whilst the pupil remains at the school, plus one year	Securely disposed of

Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Whilst the pupil remains at the school, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was not successful)	Whilst the pupil remains at the school, plus five years	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 Copies with pupils' names are held whilst the pupil is at school, plus five years Copies with pupils' names removed are held for 25 years after the pupil's date of birth	Returned to the examination board
Internal examination results	Added to the pupil's record and transferred to next school Copies with the pupil's personal data are held whilst the pupil is at school, plus five years 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	Securely disposed of

	Copies are held whilst the pupil is at school, plus one year	
Exclusion records	Added to the pupil's record and transferred to the next school 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	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth	Securely disposed of – shredded
Attendance		
Attendance registers	Whilst the pupil remains at school, plus one year Non-identifiable summary statistics are held after the initial retention period for 25 years after the pupil's date of birth	Securely disposed of
Letters authorising absence	Whilst the pupil remains at school, plus one year Non-identifiable summary statistics are held after the initial retention period for 25 years after the pupil's date of birth	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 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 Copies held whilst the pupil is at school, plus 25 years	Securely disposed of
SEND		
SEND files, reviews and individual education plans	25 years after the pupil's date of birth (as stated on the pupil's record)	Information is reviewed and the file may be kept for longer than necessary if it is required for the school to defend themselves in a 'failure to provide sufficient education' case
An EHC plan maintained under section 37 of the Children and Families Act 2014 (and any amendments to the statement or plan)	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Information and advice provided to parents regarding SEND	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Accessibility strategy	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of, unless it is subject to a legal hold
Curriculum management		
SATs results	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 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
Walking bus registers	Three years from the date of the register being taken	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
Parents NI number	Whilst the pupil is at school, plus one month	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	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
Recruitment		
Records relating to the appointment of a new headteacher	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of

Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file and other information retained for six months	Securely disposed of
DBS certificates	Details such as certificate numbers and date of clearance to be entered on the SCR then DBS disposed of immediately. Any RA associated with a DBS to be kept for as long as the staff member/volunteer is attending the school plus six years. Supply or outside agencies DBS will be kept for as long as they are attending the school.	Securely disposed of
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, 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 If allegations are malicious, they are removed from personal files	Reviewed and securely disposed of – shredded
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	If unable to store, these will be provided to the county archives service
Inspection copies of the minutes of governing board meetings	Date of meeting, plus three years	Shredded if they contain any sensitive and personal information
Reports presented to the governing board	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed, original copy of minutes
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	If unable to store, these will be provided to the county archives service

Trusts and endowments managed by the governing board	Permanent	Retained in the school whilst it remains open, then provided to the county archives service when the school closes
Action plans created and administered by the governing board	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the governing board	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the governing board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports created under the requirements of The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002	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
Headteacher and senior leadership team (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 county archives service if appropriate
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the headteacher or SLT	Date of the report, plus a minimum of three years	Reviewed and securely disposed of
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 and securely disposed of
Correspondence created by the headteacher, deputy headteacher, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Reviewed and securely disposed of
Professional development plan	Duration of the plan, plus six years	Securely disposed of

School development plan	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, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	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 radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	Current academic year, plus six years	Securely disposed of

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
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
Accounts and statements including budget management		
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	Current financial year, 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	Current academic year, plus two 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 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. 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	Current academic year, plus six years	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	Current academic year, plus six years	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 publication of the school brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards
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	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year, 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

10. Identifying information

10.1. 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.

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

10.3. 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.

10.4. 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.

11. Storing and protecting information

11.1. The DPO will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.

11.2. 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.

11.3. Where possible, backed-up information will be stored off the school premises, using a central back-up service operated by the LA.

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

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

11.6. 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.

11.7. 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.

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

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

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

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

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

11.13. Emails containing sensitive or confidential information are password-protected to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

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

11.15. Confidential information will not be sent by fax.

11.16. 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.

11.17. 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.**

11.18. 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.

11.19. 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.

11.20. 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.

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

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

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

12. Accessing information

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

12.2. 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.**

12.3. 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.

12.4. 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.

12.5. 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.

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

13. Digital continuity statement

13.1. Digital data that is retained for longer than six years will be named as part of a digital continuity statement.

13.2. The DPO will identify any digital data that will need to be named as part of a digital continuity statement.

13.3. 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 11 of this policy.

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

13.5. The IT technician will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

13.6. The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

14. Information audit

14.1. The school conducts information audits on an annual basis 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

14.2. 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

14.3. 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

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

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

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

15. Disposal of data

15.1. 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.

15.2. 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. 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.

15.3. 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.

15.4. 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.

15.5. 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.

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

16. Monitoring and review

16.1. 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 2019.

16.2. 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.

17. 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.

18. 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.

19. 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